ADMINISTRATION GUIDE

Cisco Small Business Pro

IP Phones Models SPA 501G, 502G, 504G, 508G, 509G, 525G, and WIP310

OL-19749-03

Contents

1

Getting Started

This chapter contains basic information on Cisco SPA 500 Series and Wireless-G IP Phones. It includes the following sections:

Overview of the Phones

The Cisco SPA 500 Series and Wireless-G IP Phone family is a line of full-featured VoIP (Voice over Internet Protocol) phones that provide voice communication over an IP network. They provide all the features of traditional business phones, such as call forwarding, redialing, speed dialing, transferring calls, conference calling and accessing voice mail. Calls can be made or received with a handset, a headset, or a speaker.

The Cisco SPA 500 Series and Wireless-G IP Phone family includes the models shown in the following table:

Model	Screen	Lines	Softkeys	Navigation Button
SPA 501G	Paper labels	8	4 fixed (forward, cancel, conference, and transfer)	No
SPA 502G	128 X 64 monochrome LCD with backlight	1	4 dynamic	Four-way navigation key
SPA 504G		4		
SPA 508G		8		
SPA 509G		12		
SPA 525G	320 X 240 color high-resolution LCD with backlight	5		Four-way navigation key with center-select button
WIP310	128 X 160 color with backlight	1	None	

For more information on phone features, see the data sheets for each product.

Cisco SPA 500S Attendant Console

The Cisco SPA 500S Attendant Console is used with the Cisco SPA 500 Series IP Phone models to provide additional lines. The Cisco SPA 500S has 32 LEDs/buttons for dialing, call transfer, call pick up and call monitoring. Multi-colored LEDs monitor the status of each configured voice line via busy lamp field (BLF). You can attach two attendant consoles to an IP phone, for 64 LEDs/buttons. For more information, see **Chapter 9, "Configuring the Cisco SPA 500S Attendant Console."**

Network Configurations

The Cisco SPA 500 Series and Wireless-G IP Phones support Session Initiation Protocol (SIP) or Smart Phone Control Protocol (SPCP). SPCP is supported only on the Cisco SPA 500 Series IP Phones.) You can use the Cisco SPA 500 Series and Wireless-G IP Phones as part of a Cisco SPA 9000 Voice System phone network, or with any vendor's IP PBX system that supports SIP. The Cisco SPA 500 Series IP phones can be used as part of a Cisco SPA 9000 Voice System phone network, a SIP network, or as part of the Cisco Unified Communications 500 Series for Small Business.

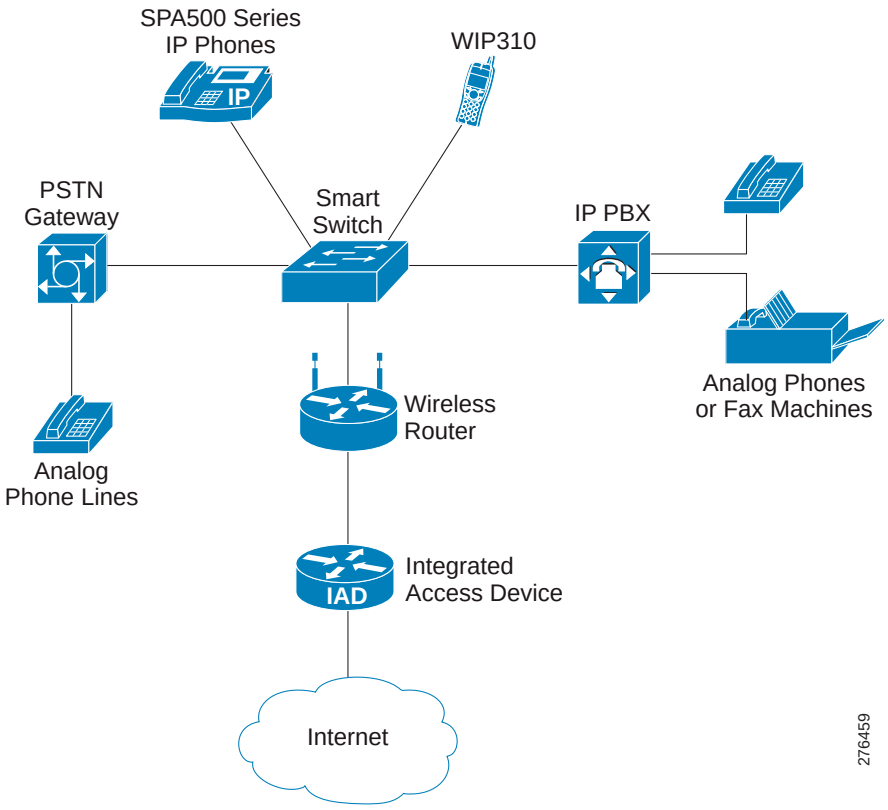


Figure 1 Network Configuration Example

NOTE Using the Cisco SPA 500 Series and Wireless-G IP Phones as part of a Cisco SPA 9000 Voice System Network provides seamless integration of advanced features, such as paging, call pickup, and shared line appearances.

This document describes some common network configurations; however, your configuration may vary depending on the type of equipment used by your service provider.

Cisco SPA 9000 Voice System

The Cisco SPA 9000 Voice System is an affordable and feature-rich voice over IP (VoIP) telephone system that is designed especially for small businesses. The Cisco SPA 9000 Voice System uses standard TCP/IP protocols and can provide global connectivity through any Internet Telephony Service Provider (ITSP) that supports SIP.

At minimum, the Cisco SPA 9000 Voice System includes a Cisco SPA 9000 IP PBX and one or more Cisco SPA 500 Series or Wireless-G IP Phones. These devices are connected through a switch to a local area network. With an Internet connection, the Cisco SPA 9000 Voice System can subscribe to ITSP services to take advantage of low calling rates. With the optional Cisco SPA 400, the Cisco SPA 9000 Voice System can connect to the Public Switched Telephone Network (PSTN) to support legacy phone lines. The Cisco SPA 400 also provides local voice mail service.

When you use Cisco SPA 500 Series and Wireless-G IP Phones with the Cisco Cisco SPA 9000 Voice System, the following additional phone features are available:

- Auto attendant for multiple extensions
- Music on hold
- Configurable call routing
- Multiple DID numbers per VoIP line
- Call hunting (sequential, round robin, random)
- Group paging
- Call parking
- Call pick up
- Group call pick up

You can configure and manage the Cisco SPA 9000 Voice System using an Interactive Voice Response (IVR) system, the Cisco SPA 9000 Voice System Setup Wizard, or a built-in web server. For more information, see the *Cisco SPA 9000 Voice System Administration Guide.*

Cisco Unified Communications 500 Series for Small Business

The Cisco Unified Communications 500 Series for Small Business is an affordable appliance that provides voice, data, voice mail, Automated Attendant, video, security, and wireless capabilities while integrating with existing desktop applications such as calendar, e-mail, and customer relationship management (CRM) programs. The Cisco SPA 500 Series IP Phones can be configured to work with this system.

Other SIP IP PBX Call Control Systems

The Cisco SPA 500 Series and Wireless-G IP Phones are compatible with other IP PBX call control systems, such as BroadSoft and Asterisk, that use SIP for call processing. Configuration of those systems is not covered in this document. Additional resources for configuring the Cisco SPA 500 Series and Wireless-G IP Phones to work with these systems are available in **Appendix C, "Where to Go From Here."**

Prerequisites

This document assumes that you have performed the following prerequisites before administering your Cisco SPA 500 Series and Wireless-G IP Phones. If you have not completed these prerequisites, see the documentation in **Appendix C, "Where to Go From Here."** for more information.

1. Set up your IP network.
2. Configure the wireless network (required for Cisco SPA 525G and WIP310).
3. Install and configure the call control system, such as such as a Cisco SPA Cisco SPA 9000, Cisco Unified Communications 500 Series for Small Business, or an Internet-based IP PBX.
4. Update firmware. See **Upgrading Firmware, page 7**.

Upgrading Firmware

Phones should be upgraded to the latest firmware before using any administration features. There are various ways to upgrade your firmware:

All Phones

- Cisco SPA 9000 Voice System Setup Wizard—If you are using the Cisco SPA 500 Series and Wireless-G IP Phones with a Cisco SPA 9000, you can use the Cisco SPA 9000 Voice System Setup Wizard to upgrade your phones. See the *Cisco SPA 9000 Voice System Setup Wizard User Guide*.
- Autoprovisioning—A configuration file that includes upgrade information is downloaded by a user's phone when it is powered on. See the **"Upgrading, Resyncing, and Rebooting Phones" section on page 139**.

Cisco SPA 50XG and WIP310

- Firmware Upgrade Executable File (Cisco SPA 50X or WIP310)—Download the firmware upgrade utility from the product page on Cisco.com to your PC desktop and run the upgrade from your PC by double-clicking the executable file. Your computer must be on the same network as the Cisco SPA 500 Series and Wireless-G IP Phone.

Cisco SPA 525G

- Web Interface (Cisco SPA 525G)—You can download the latest firmware onto your PC desktop and use the web interface to upgrade your firmware.

WIP310

- TFTP/HTTP server—The latest firmware image file is loaded onto an HTTP/TFTP server and is accessed by a web browser. See the *Cisco WIP310 User Guide* for more information.

Determining the Current Firmware Version

Before upgrading, determine the current firmware version:

Cisco SPA 501G:

STEP 1 Press the **Setup** button.

STEP 2 In the IVR menu, enter **150**, then press **#**. The firmware version is recited.

Cisco SPA 502G, Cisco SPA 504G, Cisco SPA 508G, Cisco SPA 509G:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Product Info** and then press **Select**. The current firmware is displayed under *Software Version*.

Cisco SPA 525G:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Status** and press **Select**.

STEP 3 Select **Product Information**. The current firmware is displayed under *Software Version*.

WIP310

STEP 1 In the **Home** screen, press the **Options**, highlight *Phone Info*, and press the **Select** button.

STEP 2 Scroll to *Software Version*.

Determining Your IP Address

Before you upgrade, you'll need the IP address of the phone you are upgrading. To get your IP address:

Cisco SPA 501G:

STEP 1 Press the **Setup** button.

STEP 2 In the IVR menu, enter **110**, then press **#**. The IP address is recited.

Cisco SPA 502G, Cisco SPA 504G, Cisco SPA 508G, Cisco SPA 509G:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Network** and press **Select**. The IP Address is displayed under Current IP.

Cisco SPA 525G:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Status** and press **Select**.

STEP 3 Scroll to **Network Status** and press **Select**. The IP address of your phone is displayed.

WIP310:

STEP 1 In the Home screen, press the **Select** key and navigate to *Settings*.

STEP 2 Press the **Select** key and navigate to **Phone Info**.

STEP 3 The **IP Address** section displays the IP address.

Downloading the Firmware

NOTE Requires a Cisco.com user ID and password.

STEP 1 Direct your browser to the following URL: http://www.cisco.com/public/sw-center/index.shtml.

STEP 2 Search to locate your product.

STEP 3 Locate the download page and download the firmware file.

STEP 4 If the firmware file you download is in zip format, double-click the file and extract its contents to a single folder or to the desktop.

Installing the Firmware

NOTE Your computer must be on the same sub-network as the phone you are upgrading.

Cisco SPA 50XG:

STEP 1 Run the executable file for the firmware upgrade.

STEP 2 Click **Continue** after reading the message regarding upgrading and your service provider.

STEP 3 Enter the IP address of your phone.

STEP 4 Follow the on-screen directions.

Cisco SPA 525G

STEP 1 Log in to the web interface for the phone.

STEP 2 Choose the **Firmware Upgrade** tab.

STEP 3 Click **Firmware Upgrade Window**.

STEP 4 Browse to select the firmware file from your PC. Click **Submit**. The firmware is installed and your phone reboots.

WIP310

STEP 1 Turn off your WIP310 and connect it to your computer by using the USB cable.

STEP 2 Double-click the executable file for the firmware upgrade (for example, double-click **wip310-5-0-11.exe**).

STEP 3 Follow the on-screen instructions.

STEP 4 When the upgrade is complete, disconnect the phone from your PC and power it on.

Using the Web Administration User Interface

You must be connected to the same network as your phone. For example, if you are connected to a VPN, you must first disconnect.

NOTE If you are using the Cisco SPA 500 Series IP Phones with the Cisco Unified Communications 500 Series for Small Business for Call Control, use Cisco Unified Communication Manager Express or Cisco Configuration Assistant for phone administration. For more information, refer to the *Cisco Unified Communications 500 Office Administrator Guide*.

To access the IP phone administration web user interface (UI):

STEP 1 Launch a web browser on a computer that can reach the phone on the network.

STEP 2 Direct the browser to the IP address of the phone. To determine the IP address:

- Cisco SPA 502G, Cisco SPA 504G, Cisco SPA 508G, Cisco SPA 509G: Press the **Setup** button, then select **Network**. The *Current IP* field shows the phone's current IP address.
- Cisco SPA 501G: Press the **Setup** button. In the IVR menu, enter **110**, then press **#**. The IP address is recited.
- WIP310: In the **Home** screen, press **Options** and highlight *Phone Info*. Press the **Select** button.
- Cisco SPA 525G: Press the **Setup** button, then select **Status**. Select *Network Status*. The IP address is displayed.

STEP 3 Enter the IP address in your web browser address bar. For example:

```
http://192.168.1.8
```

NOTE If your service provider disabled access to the web UI, you must contact the service provider.

If you have trouble accessing the web interface, perform the following steps:

Cisco SPA 502G, Cisco SPA 504G, Cisco SPA 508G, Cisco SPA 509G:

STEP 1 Press the **Setup** button on the phone.

STEP 2 Select **Network**.

STEP 3 Scroll to **Enable Web Server** and make sure that it is set to **Yes**. If not, press the **Edit** soft key and press **y/n** soft key to set it to **Yes**.

STEP 4 Press **OK**, then press **Save**.

Cisco SPA 501G:

STEP 1 Press the Setup button on the phone.

STEP 2 In the IVR menu, enter 7932.

STEP 3 Press 1 to enable the web server, then press #.

STEP 4 To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press *.

WIP310:

STEP 1 In the **Home** screen, press the **Select** button to choose **Settings**.

STEP 2 Press the **Select** button again to reach the **Settings** menu.

STEP 3 Scroll to highlight *Misc Settings* and press the **Select** button.

STEP 4 Press the left arrow to ensure that **Enable Web Server** is set to **On**.

STEP 5 Press the **Select** button to save this setting.

Cisco SPA 525G:

STEP 1 Press the **Setup** button.

STEP 2 Select **Network Configuration**.

STEP 3 Scroll to **Web Server** and make sure it is set to **On**.

STEP 4 Press **Save**.

Understanding Administrator and User Views

Depending on whether you are a VAR or service provider, you might have different privileges. By default, the Administrator account name is **admin**, and the User account name is **user**. These account names cannot be changed.

If the service provider set an Administrator account password, you are prompted for it when you click **Admin Login**.

The Administrator account can modify all web profile parameters, including web parameters available to the user login. The Administrator specifies the parameters that a User account can modify using the **Provisioning** tab of the web UI.

NOTE No default passwords are assigned to either the Administrator or User accounts. Only the Administrator account can assign and change passwords.

Accessing Administrative Options

To access administrative options, either:

- Log in to the web interface, then click **Admin Login**.
- Enter the following URL when accessing the interface:

  `http://phone.ip.address/admin/`

NOTE To save changes on a web page, click **Submit All Changes** before switching between User and Admin Login or between basic and advanced views. Switching logins or views discards any unsubmitted changes.

Understanding Basic and Advanced Views

These views are similar, but *advanced* view shows more options on each web page. To see all available options for your login, use the *advanced* view.

Using the Web Administration Tabs

Each tab contains different parameters. Some tasks require you to set parameters in different tabs.

For field reference about each parameter available on the web UI, see **Appendix B, "Cisco SPA 500 Series and Wireless IP Phone Field Reference."**

Roadmap to Web UI Features

The following tables provide a roadmap to features available on the web UI.

To perform these tasks...	On the web UI, click the ...
View phone, extension, and line/call information, including: ▪ DHCP, current IP address, DNS addresses ▪ Software and hardware versions ▪ Broadcast, RTP, and SIP information ▪ Registration state ▪ Packets sent, received, lost, and other information	**Info** tab See **"Viewing Phone Information" section on page 17**.
Configure system-level parameters, including network and debug parameters. To: ▪ Enable the web UI and web administrator access ▪ Set the Internet connection type to DHCP ▪ Configure the syslog and debug servers ▪ Enable VLAN and CDP	**System** tab See **Chapter 5, "Configuring Security, Quality, and Network Features."**

To perform these tasks...	On the web UI, click the ...
Configure parameters to adjust SIP stack and protocols. To enable: ▪ CTI ▪ SIP-B ▪ STUN	**SIP** tab See **Chapter 4, "Configuring SIP, SPCP, and NAT."**
Configure provisioning parameters. To: ▪ Enable remote provisioning ▪ Enable firmware upgrades ▪ Set general purpose parameters	**Provisioning** tab The *Provisioning* tab is viewable by Admin logins only. See **Chapter 6, "Provisioning Basics."** For additional information about provisioning, see the *Cisco Small Business IP Telephony Devices Provisioning Guide* (for Cisco service providers).
Configure parameters that depend on country or region, including: ▪ Call progress tones ▪ Ring patterns ▪ Star codes/vertical service activation codes ▪ Vertical service announcement codes ▪ Local date/time and language	**Regional** tab See **Chapter 7, "Configuring Regional Parameters and Supplementary Services."**
Configure General phone station info, which applies to all extensions configured for the phone, including: ▪ Station name, voice mail number, text logos and background pictures ▪ Extension numbers for line keys ▪ Shared call (line) appearance ▪ Enabling call conferencing, call forward, call transfer, and so on. ▪ Select ring tones, audio input, and extension mobility settings	**Phone** tab See **Chapter 3, "Customizing Cisco SPA and Wireless IP Phones."**

To perform these tasks...	On the web UI, click the ...
Customize individual extension parameters, including: ▪ Shared line/call appearance ▪ NAT settings ▪ SIP settings such as SIP debug and SIP port ▪ Mailbox ID, MOH server ▪ Voice mail server ▪ Proxy and registration information ▪ Subscriber information such as user ID and password ▪ Audio settings ▪ Dial plan settings	**Ext** tab (1-6, depending on phone model) See **Chapter 2, "Configuring Lines and Extensions."**
Customize user-level parameters, including: ▪ Call forward ▪ Speed dial ▪ Supplementary services ▪ Web information (RSS newsfeeds) ▪ Traffic information settings ▪ Audio volume ▪ Phone GUI settings	**User** tab See **Chapter 3, "Customizing Cisco SPA and Wireless IP Phones."**
View and change parameters for Unit 1 and Unit 2 (applicable only to Cisco SPA 500 Series IP Phones with one or two Cisco SPA 500S attendant consoles attached)	**Attendant Console** tab See **Chapter 9, "Configuring the Cisco SPA 500S Attendant Console."**

Viewing Phone Information

After you log on to the web UI (see **"Using the Web Administration User Interface" section on page 11**), you can check the current status of the Cisco SPA 500 Series or Wireless-G IP Phone by clicking the **Info** tab. The Info tab shows information about all phone extensions, including phone statistics and the registration status. All fields are read-only.

See **"Info Tab" section on page 197** for more information about the fields.

Using IVR on the Cisco SPA 501G IP Phone

The Cisco SPA 501G provides an IVR menu to perform configuration tasks and obtain information about the phone.

To access the IVR menu, press the **Settings** button. Enter the number of the option and press #. Some menus require entering of further information or numbers.

You have the following options:

Number	Option
100	Tells you if Dynamic Host Configuration Protocol (DHCP) is enabled.
110	Recites the IP address of the phone.
120	Recites the netmask of the phone.
130	Recites the gateway address.
140	Recites the MAC (hardware) address of the phone.
150	Recites the phone software version.
160	Recites the primary DNS server address.
170	Recites the HTTP port on which the web server listens. Defaults to 80.
180	Recites the IP multicast address (used by the Cisco SPA 9000 to communicate with the IP phone).
220	Recites the method of call control (SIP or SPCP).

Number	Option
221	Set call control—enter the value for the call control method you want, then press #: ▪ 0: SIP ▪ 1: SPCP To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.**
73738	Restore the phone to the factory default software and settings. Enter **1** to confirm, or * to exit. If you chose to reset, hang up to exit and begin the restore process.
87778	Restore the phone's user settings to the default. (Clears all user settings such as speed dials.) Enter **1** to confirm, or * to exit. If you chose to reset, hang up to exit and begin the restore process.
732668	Reboot the phone. After entering **#**, hang up to begin rebooting.
111	Set a static IP address. Enter the address (use * to enter the "." value), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.** **NOTE** DHCP must be disabled to use this option; if DHCP is not disabled, you receive an error message.
121	Set a netmask. Enter the address (use * to enter the "." value), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.** **NOTE** DHCP must be disabled to use this option; if DHCP is not disabled, you receive an error message.
131	Set a gateway. Enter the address (use * to enter the "." value), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.** **NOTE** DHCP must be disabled to use this option; if DHCP is not disabled, you receive an error message.
161	Set the address of the primary Domain Name Server (DNS). Enter the address (use * to enter the "." value), then press #. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.**

Number	Option
181	Set the IP multicast address (used by the Cisco SPA 9000 to communicate with the IP phone). Enter the address (use * to enter the "." value), then press #. To save, press **1**. To review the value you entered, press **2**. To re-enter, press **3**. To exit, press ***.**
7932	Enable or disable the web server. Press **1** to enable or **0** to disable, then press **#**. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.**
723646	Enable or disables access to the administrative (admin) login on the web interface. Press **1** to enable or **0** to disable, then press **#**. To save, press **1**; to review, press **2**; to re-enter, press **3**; to exit, press ***.**

2

Configuring Lines and Extensions

This chapter contains the following sections:

Configuring Lines

The Cisco SPA 500 series and Wireless-G IP Phones (also called *stations* in this document) provide different numbers of lines depending on the phone model. See the **"Overview of the Phones" section on page 2** for more information.

Each line corresponds to a phone number (or extension) used for calls. Each line can support two calls. So, for example, a four-line phone can handle eight calls. One call can be active (in conversation) and seven can be on hold.

Shared Line Appearances

Shared Line Appearance (SLA) allows multiple phones to share an extension number and manage a call as a group. At any given time, each station sharing a call appearance can monitor the state of the call appearance. A station can select a shared call appearance to make a call only if the call appearance is not being used by another station.

When a call is made to the extension number for the SLA, all sharing stations ring. Any station can answer the call. If the active phone places the call on hold, the call can be resumed from any of the sharing stations by pressing the corresponding line key from another phone (Cisco SPA 500 series, except for the Cisco SPA 502G) or the **Select** button when the **Resume** icon is displayed (WIP310).

NOTE The Cisco SPA 500 Series IP Phones support the “private hold” feature for MetaSwitch and BroadSoft. Users who have a shared line can press the “**PrivHold**” softkey, and the call can only be resumed by the user who placed the call on hold.

Each station with an SLA can be configured independently. Although the account information is usually the same for all of the stations, settings such as the dial plan or the preferred codec can vary.

Configuring a Line

NOTE This section does not apply to the WIP310.

To configure a phone line:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under each line key for the phone, configure the following:

- Extension—Assign an extension to the line key. Defaults to 1. Generally you should reserve **EXT 1** on the client station as the primary and private extension of the designated user. Configure shared extensions on **EXTs 2** through **6** (depending on phone model).
- *Short Name*—Enter a short name or number to display on the LCD for the line key.
- *Share Call Appearance*—Select **shared** if you want the line key to share incoming call appearances with other phones. See **Configuring Shared Line Appearance, page 22**. If you select **private**, the call appearance is private and not shared with any other phone. Defaults to private.
- Extended Function—See **Assigning Busy Lamp Field, Call Pickup, and Speed Dial Functions to Unused Lines on a Cisco SPA 500 Series IP Phone, page 23**.

NOTE The number of line keys displayed depends on the type of phone.

STEP 5 Click **Submit All Changes**.

Configuring Shared Line Appearance

After configuring the line and choosing **shared** in the Shared Call Appearance field, perform the following steps:

STEP 1 Click the **Ext** <number> tab of the extension that is shared (do not use Ext 1).

STEP 2 Under **General**, in the **Line Enable** field, choose **yes**.

STEP 3 Under **Share Line Appearance**, in the **Share Ext** field, select **shared**. If you set this extension to private (not shared), the extension does not share calls, regardless of the **Share Call Appearance** setting on the **Phone** tab. If you set this extension to **shared**, calls follow the **Share Call Appearance** setting on the **Phone** tab. On the Cisco SPA 50XG phones that have line buttons, a hollow telephone icon is displayed next to the shared line button. For the Cisco SPA 525G, a telephone icon is displayed.

STEP 4 In the **Shared User ID** field, enter the user ID (name) of the phone with the extension that is being shared.

STEP 5 (Optional) In the **Subscription Expires** field, enter the number of seconds before the SIP subscription expires. Before the subscription expiration, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension. The default is 60 seconds.

STEP 6 Under **Proxy and Registration**, in the **Proxy** field, enter the IP address of the proxy server (for example, the IP address of the Cisco SPA 9000).

STEP 7 Under **Subscriber Information**, enter a **Display Name** and **User ID** (extension number) for the shared extension. These are shown on the phone screen.

STEP 8 (Optional) In the **Phone** tab, under **Miscellaneous Line Settings**, you can configure line mapping. Each LED (line/extension) can hold two calls. You can assign an extension to two LEDs. The first call always causes the assigned LED to flash. Choose one of the following:

- Vertical first—The next LED on the phone flashes with the second incoming call.
- Horizontal first—The same LED to flashes with the second incoming call.

STEP 9 (Optional) Under **SCA Barge-In Enable**, choose **yes** to allow users sharing call appearances to take over the call on a shared line.

For example, Bob and Chris share the extension 401. A caller, Adam, calls extension 401. Bob answers the call. Adam and Bob are connected. If Chris has the SCA Barge-In Enable field on her phone set to **yes**, she can press the line button for extension 401. Then Chris and Adam are connected in a call and Bob is dropped from the call.

NOTE The Cisco SPA 525G supports the "private hold" feature for MetaSwitch and Broadsoft. Users who have a shared line can press the "**PrivHold**" softkey, and the call can only be resumed by the user who placed the call on hold. No barge-in can be performed on these calls.

STEP 10 Click **Submit All Changes**.

Assigning Busy Lamp Field, Call Pickup, and Speed Dial Functions to Unused Lines on a Cisco SPA 500 Series IP Phone

You can configure unused or idle lines on a Cisco SPA 500 Series IP Phone to interact with another phone line in the system. For example, if you have two idle lines on an assistant's phone, you can configure those lines to show the status of a supervisor's phone (Busy Lamp Field, or BLF). You can also configure the idle lines so that they can be used to speed dial the supervisor's phone, or pick up calls that are ringing on the supervisor's phone.

NOTE A monitored extension must be private, not shared. Additionally, an extension can only be monitored by one other extension.

Configuring Call Pickup and Busy Lamp Field

NOTE You must enable BLF to configure call pickup.

In this example, the assistant Bob (extension 200) has an idle line (line 4) on his Cisco SPA 508G. He would like to be able to see if his supervisor Stephanie (extension 300) is on the phone, and pick up calls that are ringing at her extension.

To configure this feature for Bob's Cisco SPA 508G:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login**.

STEP 3 Click **advanced**.

STEP 4 Click the **Phone** tab.

STEP 5 Find the first line to configure (line 4 in this example):

a. From the *Extension* drop down list, choose **Disabled**.

b. From the *Share Call Appearance* drop-down list, choose **private**.

c. Enter the following string in the Extended Function field:

```
fnc=blf+cp;sub=Stephanie@$PROXY;ext=300@$PROXY
```

Using the following syntax:

```
fnc=type;sub=stationname@$PROXY;ext=extension#@$PROXY
```

where:

- fnc: function
- blf: busy lamp field
- cp: call pickup
- sub: station name
- ext or usr: extension or user (the usr and ext keywords are interchangeable)

STEP 6 Click **Submit All Changes**. After the phone reboots, the phone (in this example) should show the following color LEDs for the monitored lines:

- Green: Available
- Red: Busy
- Red Fast Blink: Ringing

If the phone LEDs display orange or slow blinking orange, there is a problem: Orange denotes that the phone failed to subscribe (received 4xx response) and slow blinking orange denotes an undefined problem (there may be no response to subscribe, or BLF).

In this example, after this configuration, Bob will be able to monitor Stephanie's line. He can press line button 4 to pick up a call ringing at Stephanie's line.

Configuring Speed Dial

In this example, the assistant Bob (extension 200) has another idle line (line 5) on his Cisco SPA 508G. He would like to be able to speed dial his supervisor Mark (extension 400) from that line.

To configure this feature for Bob's Cisco SPA 508G:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login**.

STEP 3 Click **advanced**.

STEP 4 Click the **Phone** tab.

STEP 5 Find the first line to configure (line 5 in this example):

a. From the *Extension* drop down list, choose **Disabled**.

b. From the *Share Call Appearance* drop-down list, choose **private**.

c. Enter the following string in the Extended Function field:

`fnc=sd;ext=400@$PROXY`

Using the following syntax:

`fnc=type;ext=extension#@$PROXY`

where:

- fnc: function

- sd: speed dial
- ext or usr: extension or user (the usr and ext keywords are interchangeable)

STEP 6 Click **Submit All Changes**.

In this example, after this configuration, Bob can press line button 5 to dial Mark's line.

Configuring Unused Line Keys for Call Park on the Cisco SPA 525G (MetaSwitch)

You can configure unused line keys for call park (for the MetaSwitch softswitch) on the Cisco SPA 525G. Users can then press this line button to park a call or retrieve a parked call. To configure:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login**.

STEP 3 Click **advanced**.

STEP 4 Click the Attendant Console tab. In the *General* section, under *Server Type*, choose **RFC3265_4236**.

STEP 5 Click the **Phone** tab.

STEP 6 Choose the line key to configure (line 5 in this example):

a. From the *Extension* drop down list, choose **Disabled**.

b. From the *Share Call Appearance* drop-down list, choose **private**.

c. Enter the following string in the Extended Function field:

```
fnc=prk;sub=05@domain.com
```

where:

- fnc: function
- prk: call park
- sub: call park orbit, or location where the call is parked. Valid value range is from 01 through 10. In this example, 5 is used.

- domain.com: phone domain, usually the same as the “proxy” value in the Ext 1 tab. You can also use fnc=prk;sub=05@$PROXY to use this value.

STEP 7 Click **Submit All Changes**.

Configuring Unused Line Keys to Access Services

On the Cisco SPA 500 Series IP Phones, unused or idle phone lines can also be configured to access services, such as the following:

- XML services
- MP3 player
- Weather (RSS)
- News (RSS)

To configure line keys to access services:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login**.

STEP 3 Click **advanced**.

STEP 4 Click the **Phone** tab.

STEP 5 Find the first line to configure (line 4 in this example):

a. From the *Extension* drop down list, choose **Disabled**.

b. Enter the following string in the Extended Function field:

`fnc=type`

where:

- fnc: function
- type: choose from the following:
  - xml: pressing the line button accesses XML services.

NOTE The XML service configured on the Phone tab under the XML Service field is used (see the **"Configuring XML Services" section on page 73**). You can specify a different XML service to connect to by using the syntax "fnc=xml;URL=http://xxx.xx.xxx/entry.html" where xxx.xx.xxx is the URL of the XML service.

- mp3: pressing the line button starts the mp3 player.
- weather: pressing the line button accesses weather information.
- news: pressing the line button accesses news.

For example, to configure line 4 for the mp3 player:

```
fnc=mp3
```

STEP 6 Click **Submit All Changes**. After the phone reboots, configured lines glow orange and display the following icons next to the extension label:

- xml: XML icon
- mp3: mp3 player icon
- news: RSS icon
- weather: thermometer icon

Configuring Line Key LED Patterns on the Cisco SPA 500 Series IP Phone

You can customize the LED patterns for the line keys on the phone by entering letters for the color or pattern in the LED pattern fields.

To configure Line Key LED patterns:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Line Key LED Pattern**, use the following letters to customize the fields shown in the following table:

- "p" indicates "pattern": the blinking pattern of the LED
- "c" indicates "color": the color of the LED
- "r" indicates "red": a red-colored LED
- "g" stands for "green": a green-colored LED

Parameters	Description
Idle LED	Appears when the line is idle. Defaults to blank (c=r).
Remote Undefined LED	LED pattern during the Remote Undefined state, where the shared call state is undefined (the station is still waiting for the state information from the application server). Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Seized LED	Appears when this station seizes the call appearance to prepare for a new outbound call. Defaults to blank (c=r).
Remote Seized LED (applicable only to shared call appearance)	Appears when the shared call appearance is seized by another station. Defaults to blank (c=r; p=d).
Local Progressing LED	Appears when this station attempts an outgoing call on this call appearance (the called number is ringing). Defaults to blank (c=r).
Remote Progressing LED (applicable only to shared call appearance)	Appears when another station attempts an outbound call on this shared call appearance. Defaults to blank (c=r; p=d).
Local Ringing LED	Appears when the call appearance is ringing. Defaults to blank (c=r;p=f).

Parameters	Description
Remote Ringing LED (applicable only to shared call appearance)	Appears when the shared call appearance is in ringing on another station. Defaults to blank (c=r;p=d).
Local Active LED	Appears when the call appearance is engaged in an active call. Defaults to blank (c=r).
Remote Active LED (applicable only to shared call appearance)	Appears when another station is engaged in an active call on this shared call appearance. Defaults to blank (c=r;p=d).
Local Held LED	Appears when the call appearance is held by this station. Defaults to blank (c=r;p=s).
Remote Held LED (applicable only to shared call appearance)	Appears when another station places this call appearance on hold. Defaults to blank (c=4,p=s).
Register Failed LED	LED pattern when the corresponding extension has failed to register with the proxy server. Leaving this entry blank indicates the default value of c=a.
Disabled LED	LED pattern when the Call Appearance is disabled (not available for any incoming or outgoing call). Leaving this entry blank indicates the default value of c=o.
Registering LED	Appears when the corresponding extension tries to register with the proxy server. Defaults to blanks (c=r;p=s).
Call Back Active LED	Indicates Call Back operation is currently active on this call. Defaults to blank (c=r;p=s).

STEP 5 Click **Submit All Changes**.

For more information on LEDs, see the **"Creating an LED Script" section on page 193**.

Configuring Extensions

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Ext** <number> tab for the extension you want to configure.

STEP 4 In the **General** section, make sure that **Line Enable** is set to **yes**.

You can configure many parameters differently for different extensions. These parameters are grouped on the **Ext** <number> tab. These parameters are explained in other sections of this document:

- NAT, Network, and SIP Settings—**Chapter 4, "Configuring SIP, SPCP, and NAT."**
- Call Feature Settings—**Chapter 3, "Customizing Cisco SPA and Wireless IP Phones."**
- Proxy and Registration—**Chapter 4, "Configuring SIP, SPCP, and NAT."**
- Subscriber Information—**Chapter 4, "Configuring SIP, SPCP, and NAT."**
- Audio (Codec) Configuration—**Chapter 5, "Configuring Security, Quality, and Network Features."**
- Dial Plan—**Chapter 3, "Customizing Cisco SPA and Wireless IP Phones."**

3

Customizing Cisco SPA and Wireless IP Phones

This chapter describes customizing the SPA 500 Series and Wireless-G IP phones and contains the following sections:

Configuring Phone Information and Display Settings

The web administration interface allows you to customize the phone and configure settings such as the phone name, background photo, logo, and screen saver.

Configuring the Phone Name

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **General**, enter the Station Name, or name for the phone. This name shows up in the corporate directory.

STEP 5 Click **Submit All Changes**. The phone reboots.

Configuring Voice Mail

To configure the phone to connect to voice mail:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **General**, enter the Voice Mail Number. This is the internal or external phone number or URL to access the voice mail system. If using an external voice-mail service, the number must include any digits required to dial out and any required area code.

STEP 5 Click **Submit All Changes**. The phone reboots.

Configuring Internal Voice Mail for Each Extension (When Using Cisco SPA 400 for Voice Mail)

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Ext** <number> tab.

STEP 4 Under **Call Feature Settings**, enter the voice mail line number and phone extension in the **Mailbox ID** field. For example, 2101 indicates that the Cisco SPA 400 voice mail server is configured on the Cisco SPA 9000 Line 2, phone extension 101.

STEP 5 Enter the IP address of the voice mail server.

STEP 6 Click **Submit All Changes**.

Customizing the Startup Screen

You can create a text logo to display when the IP phone boots up. (Not applicable to the WIP310.)

Cisco SPA 50XG:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab. In the Text Logo field, enter logo text as follows:

- Up to two lines of text
- Each line must be fewer than 32 characters
- Insert a new line character (\n) and escape code (%0a) between lines

For example, “Super\n%0aTelecom” will display:

```
Super
Telecom
```

STEP 4 Click **Submit All Changes**. The phone reboots.

Cisco SPA 525G:

STEP 1 Log in to the web administration interface.

STEP 2 **Admin Login** and **advanced**.

STEP 3 Click the **User** tab. In the Screen section, Text Logo field, enter logo text as follows:

- Up to two lines of text
- Each line must be fewer than 32 characters
- Insert a new line character (\n) and escape code (%0a) between lines

For example, “Super\n%0aTelecom” will display:

```
Super
Telecom
```

STEP 4 In the Logo Type field, select **Text Logo**.

STEP 5 Click **Submit All Changes**. The phone reboots.

Changing the Display Background (Cisco SPA 500 Series)

You can use a logo and picture to customize the background on your IP phone LCD displays. Phone models and acceptable image file types are:

- Cisco SPA 50XG: Bitmap format, 1 bit-per-pixel color, size 128 x 48 pixels.
- Cisco SPA 525G: Either .jpg format (recommended) or bitmap (1, 4, 8, 24, or 32 bits per pixel). Recommended image size is 320 x 240 pixels. Other image sizes are scaled to fit, which can cause distortion.

NOTE The phone does not reboot after you change the background image URL.

Cisco SPA 50XG:

STEP 1 Copy the image to a TFTP or HTTP server that is accessible from the phone.

STEP 2 Log in to the web administration interface.

STEP 3 Click **Admin Login** and **advanced**.

STEP 4 Click the **Phone** tab.

STEP 5 In the Select Background Picture field, select **BMP Picture**.

STEP 6 Enter the URL of the image file you want in the *BMP Picture Download URL* field. The URL must include the TFTP/HTTP server name (or IP address), directory, and filename, for example:

`tftp://myserver.mydomain.com/images/downloadablepicture.bmp`

or

`http://myserver.mydomain.com/images/downloadablepicture.bmp`

If the HTTP Refresh Timer is set in the server's response to **BMP Picture Download URL**, the phone downloads the picture from the link and displays it on the screen. The phone automatically retrieves the picture after the specified number of seconds.

STEP 7 Click **Submit All Changes**.

When the *BMP Picture Download URL* is changed, the phone compares the URL to the previous image's URL. (If the URLs are the same, the phone does not perform the download.) If the URLs are different, the phone downloads the new image and displays it (providing the *Select Background Picture* field is set to **BMP Picture)**.

Cisco SPA 525G:

STEP 1 Copy the image to an HTTP server that is accessible from the phone. (TFTP is not supported.)

STEP 2 Log in to the web administration interface.

STEP 3 Click **Admin Login** and **advanced**.

STEP 4 Click the **User** tab.

STEP 5 In the Screen section, Background Picture Type field, select **Download BMP Picture**.

STEP 6 Enter the URL of the .bmp file you want in the *BMP Picture Download URL* field. The URL must include the HTTP server name (or IP address), directory, and filename, for example:

`http://myserver.mydomain.com/images/downloadablepicture.jpg`

If the HTTP Refresh Timer is set in the server's response to **BMP Picture Download URL**, the phone downloads the picture from the link and displays it on the screen. The phone automatically retrieves the picture after the specified number of seconds.

STEP 7 Click **Submit All Changes**.

When the *BMP Picture Download URL* is changed, the phone compares the URL to the previous image's URL. (If the URLs are the same, the phone does not perform the download.) If the URLs are different, the phone downloads the new image and displays it (providing the *Select Background Picture* field is set to **Download BMP Picture)**.

Configuring the Screen Saver

You can configure a screen saver for the Cisco SPA 500 Series IP Phone. (Not applicable to WIP310.)

This option enables a screen saver on the phone's LCD. When the phone is idle for a specified time, it enters screen saver mode. (Users can set up screen savers directly using phone's **Setup** button.)

Any button press or on/off hook event triggers the phone to return to its normal mode. If a user password is set, the user must enter it to exit screen saver mode.

To configure the screen saver:

Cisco SPA 50XG:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 In the **General** section, in the **Screen Saver Enable** field, choose **yes**.

STEP 5 In the **Screen Saver Wait** field, enter the number of seconds of idle time to elapse before the screen saver starts.

STEP 6 In the **Screen Saver Icon** field, choose the display type:

- A background picture.
- The station time in the middle of the screen.
- A moving padlock icon. When the phone is locked, the status line displays a scrolling message "Press any key to unlock your phone."
- A moving phone icon.
- The station date and time in the middle of the screen.
- A blank "power save" screen."

STEP 7 Click **Submit All Changes**.

Cisco SPA 525G:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Screen**, in the **Screen Saver Enable** field, choose **yes**.

STEP 5 In the **Screen Saver Type** field, choose the display type:

- **Black Background**—Displays a black screen.
- **Gray Background**—Displays a gray screen.
- **Black/Gray Rotation**—The screen incrementally cycles from black to gray.
- **Picture Rotation**—The screen rotates through available pictures on the phone.
- **Digital Frame**—Shows the background picture.

STEP 6 In the **Screen Saver Trigger Time** field, enter the number of seconds that the phone remains idle before the screen saver turns on.

STEP 7 In the **Screen Saver Refresh Time** field, enter the number of seconds before the screen saver should refresh (if, for example, you chose a rotation of pictures).

STEP 8 Click **Submit All Changes**.

Configuring the LCD Contrast

You can configure the LCD contrast on the Cisco SPA 500 Series IP Phone. (Not applicable to the WIP310.)

To configure the contrast for the LCD screen on the phone:

Cisco SPA 50XG:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Audio Volume**, in the **LCD Contrast** field, enter a number value from 1 to 30. The higher the number, the greater the contrast on the screen.

STEP 5 Click **Submit All Changes**.

Cisco SPA 525G:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Screen**, in the **LCD Contrast** field, enter a number value from 1 to 30. The higher the number, the greater the contrast on the screen.

STEP 5 Click **Submit All Changes**.

Configuring Back Light Settings (Cisco SPA 525G)

To configure the back light settings for the LCD screen on the phone:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Screen**, in the **Back Light Enable** field, choose **yes** to enable the screen back light.

STEP 5 In the **Back Light Timer** field, enter the number of seconds of idle time that can elapse before the back light turns off.

STEP 6 Click **Submit All Changes**.

Configuring Linksys Key System Parameters

To configure the phone as part of a Linksys Key System (for use with the Cisco SPA 9000):

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **SIP** tab.

STEP 4 Configure the following fields:

- **Linksys Key System—**Enables or disables the Linksys Key System for use with the Cisco SPA 9000. Defaults to yes. See the *Cisco SPA 9000 System Administration Guide* for more details.
- **Multicast Address—**Used by the Cisco SPA 9000 to communicate with Cisco IP phones. Defaults to 224.168.168.168:6061. (For the Cisco SPA 501G, can be configured using the IVR. See the **"Using IVR on the Cisco SPA 501G IP Phone" section on page 17**.)
- **Key System Auto Discovery**—Enables or disables auto discovery of the call control server (for example, the Cisco SPA 9000). Disable this feature for teleworkers or other scenarios where multicast does not work.

- **Key System IP Address**—IP address of the call control server IP. Enter the IP address for teleworkers or other scenarios where multicast does not work.
- **Force LAN Codec**—Used with the Cisco SPA 9000. Choices are none, G.711u, or G.711a. Defaults to none.

STEP 5 Click **Submit All Changes**.

Enabling Call Features

This section describes how to enable and disable call features on the phone.

Enabling Anonymous Call and Caller ID Blocking

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Supplementary Services**, under the type of call blocking to enable, choose **yes**.

- **Block ANC**—Blocks anonymous calls.
- **Block CID**—Blocks outbound caller ID.

NOTE These features can also be configured from the **User** tab, under **Supplementary Services**.

STEP 5 Click **Submit All Changes**.

Enabling Automatic Call Distribution (ACD)

Typically used for call centers, Automatic Call Distribution (ACD) handles incoming calls and manages them based on a database of instructions. You can enable this with the SIP B parameter ("Configuring SIP" section on page 83).

Defaults to no (disabled).

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Supplementary Services**, in the **ACD Login Serv** field, choose **yes**.

STEP 5 In the **ACD Ext** field, choose the extension used for handling ACD calls. Select 1-6, depending on your phone model. Defaults to 1.

STEP 6 Click **Submit All Changes**.

Enabling Call Back

Call back is a feature that forces the phone to repeatedly try a number that has been dialed and received a busy response. The busy number is tried until the call goes through and the phone rings on the user's end.

To enable call back:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 In the **Phone** tab, under **Supplementary Services**, in the **Call Back Serv** field, choose **yes**.

STEP 5 Click **Submit All Changes**.

Enabling Call Park and Call Pickup

Call park and call pickup are features available on IP phones in a Cisco SPA 9000 system. Call park allows users to put a call on a line and make it available for another user to pick up. Call pickup allows a user to pick up a phone that is ringing at another user's phone.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Supplementary Services**, under the type of call feature to enable, choose **yes**.

- **Call Park Serv**—Enables call parking.
- **Call Pickup Serv**—Enables call pickup.

STEP 5 Click **Submit All Changes**.

Enabling Call Transfer and Call Forwarding

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Supplementary Services**, under the transfer type you want to enable, choose **yes**:

- **Attn Transfer**—Attended call transfer. The user answers the call before transferring it.
- **Blind Transfer**—Blind call transfer. The user transfers the call without speaking to the caller.

You can also enable or disable call forwarding:

- **Cfwd All**—Forwards all calls.
- **Cfwd Busy**—Forwards calls only if the line is busy.
- **Cfwd No Ans**—Forwards calls only if the line is not answered.

STEP 5 Click **Submit All Changes**.

Enabling Call Waiting

To enable call waiting:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Supplementary Services**, in the CW Setting field, choose **yes**.

STEP 5 Click **Submit All Changes**.

Enabling Conferencing

To allow the user to perform call conferencing on the phone:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Supplementary Services**, in the **Conference Serv** field, choose **yes**.

STEP 5 Click **Submit All Changes**.

Enabling Dial Assistance

Dial assistance can help users to place calls more quickly. When a user begins dialing, the phone displays a list of closely-matched phone numbers on the screen.

To enable dial assistance:

STEP 1 Click **Admin Login** and **advanced**.

STEP 2 Click the **User** tab.

STEP 3 Under **Supplementary Services**, in the **Dial Assistance** field, choose **yes**.

STEP 4 Click **Submit All Changes**.

Enabling Do Not Disturb

You can allow users to turn the Do Not Disturb feature on and off. This feature directs all incoming calls to voice mail or, if voice mail is not configured, plays a message to the caller saying the user is unavailable.

NOTE On the Cisco SPA 500 Series IP Phones, users can press the **Ignore** softkey to divert a ringing call to the forwarded destination.

To allow users to use Do Not Disturb (this is enabled by default):

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Supplementary Services**, under **DND Serv,** choose **yes**.

NOTE This feature can also be configured from the **User** tab, under **Supplementary Services**.

STEP 5 Click **Submit All Changes**.

Enabling the Missed Call Shortcut

The IP phones can display a notification that a call has been missed. (Not applicable to WIP310.) To enable this notification:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Supplementary Services**, in the **Miss Call Shortcut** field, choose **yes**.

STEP 5 Click **Submit All Changes**.

Logging Missed Calls (Cisco SPA 500 Series)

You may want to disable or enable missed call logging per extension. For example, if you have set up a line to monitor another user's line, you may want to disable missed call logging for the monitored line.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Supplementary Services**, in the **Log Missed Calls for EXT** <number> field, choose **yes**.

STEP 5 Click **Submit All Changes**.

Enabling Paging (Intercom)

The paging, or intercom feature, allows two types of paging:

Single Page

A user can directly contact another user by phone. If the person being paged has configured their phone to automatically accept pages (see **Configuring a Phone to Automatically Accept Pages, page 47**), the phone does not ring and a direct connection between the two phones is automatically established when paging is initiated.

Group Paging

Group Paging lets the user page all the client stations at once, or page groups of phones. If the client station is on an active call while a group page starts, the incoming page is ignored.

When paging occurs, the speaker on the paged stations is automatically powered on unless the handset or headset is being used.

Group page is one-way only. The paged client stations can only listen to the call from the originator.

To enable paging:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Supplementary Services**, under **Paging Serv**, choose **yes**.

STEP 5 Click **Submit All Changes**.

Configuring a Phone to Automatically Accept Pages

To configure a phone to automatically accept pages:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Supplementary Services**, in the **Auto Answer Page** field, choose **yes**.

STEP 5 Click **Submit All Changes**. The phone reboots.

Configuring Paging Groups

You can configure a phone as part of a paging group. Users can then direct pages to specific groups of phones.

Limitations:

- A phone can be a listening member of no more than two paging groups.
- No more than five paging groups can be configured on a phone.

To configure a phone as part of a paging group:

STEP 1 Log in to the web administration interface for the phone.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under Multiple Paging Group Parameters, enter the paging commands into the Group Paging Script field. The syntax is as follows:

```
pggrp=ip-address:port;[name=xxx;]num=xxx;[listen={yes|no}]];
```

Where:

- IP address: Multicast IP address of the phone that will listen for and receive pages.
- port: Port on which to page; you must use different ports for each paging group. All phones in the same paging group must use the same port number.
- name (optional): The name of the paging group.
- num: The number users will dial to access the paging group; must be unique to the group.
- listen: If the phone being configured is a listening member of the page group. A phone can be a listening member of a maximum of two groups. If no value is entered, the default is to **not listen** as a member of this group.

STEP 5 Click **Submit All Changes**.

Configuration Example

The following example sets up four paging groups: *All*, *Sales*, *Support*, and *Engineering*. Users will press 801 to send pages to all phones, 802 to send pages to phones configured as part of the Sales group, 803 to send pages to phones configured as part of the Support group, and 804 to send pages to phones configured as part of the Engineering group.

A phone that is configured with this example is a listening member of the "All" and "Sales" paging groups. That phone will automatically receive pages sent to those two paging groups.

For each Sales phone, enter the following in the **Phone** > **Multiple Paging Groups Parameters** > **Group Paging Script** field:

```
pggrp=224.123.123.121:43210;name=All; num=801;listen=yes;
pggrp=224.123.123.121:43211;name=Sales;num=802; listen=yes;
pggrp=224.123.123.121:43212;name=Support;num=803;
pggrp=224.123.123.121:43213;name=Engineering;num=804;
```

Enabling Secure Call

See **Setting Security Features, page 110**.

Enabling Service Announcements

The Service Announcements features allows a user to send announcement requests to a customer-supplied announcement server. (Not applicable to the WIP310.)

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Service Annc Serv**, choose **yes**.

STEP 5 Click **Submit All Changes**.

Configuring Phone Features

The following sections describe how to configure features on the phone such as softkeys, the message waiting indicator, ring tones, and audio features.

Customizing Phone Softkeys

NOTE This feature is unavailable on the Cisco SPA 500 Series IP Phones using SPCP.

The Cisco SPA 500 Series IP phones have four softkeys on the screen that, when pressed, perform certain actions. (The Cisco SPA 501 does not have any softkeys.)

The default softkeys (when the phone is in an idle state) are Redial, Directory, Call Forward, and Do Not Disturb. Other softkeys are available during specific call states (for example, if a call is on hold, the Resume softkey displays).

You can customize the softkeys displayed on the phone. To program softkeys:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 In the Programmable Softkeys section, under Programmable Softkey Enable, choose **yes**.

STEP 5 Edit the softkeys depending on the call state in which you want the softkey to display. See the following table for information about softkeys.

STEP 6 Click **Submit All Changes**.

In the Programmable Softkeys section, each phone state is displayed and the softkeys that are available to display during that state are listed. Each softkey is separated by a semicolon. Softkeys are shown in the format:

softkeyname|[*position*]

where *softkeyname* is the name of the key and *position* is where the key is displayed on the phone screen. Positions are numbered, with position one displayed on the lower left of the screen, followed by positions two through four. Additional positions are accessed by pressing the right arrow key on the phone. If no position is given for a softkey, the key will "float" and appears in the first available empty position on the screen.

NOTE On the Cisco SPA 525G, in the Off Hook State, the **More** softkey is fixed in position 4 and cannot be changed.

The table below lists each softkey and the phone state under which the softkey displays. You can have a maximum of 16 softkeys for each call state field.

Keyword	Key Label	Definition	Available Phone States
acd_login	Login	Logs user in to Automatic Call Distribution (ACD).	Idle
acd_logout	Logout	Logs user out of ACD.	Idle
alpha	Alpha	Enter alphabetic characters in a data entry field.	Off-Hook, Dialing Input
answer	Answer	Answers an incoming call.	Ringing
avail	Avail	Denotes that a user who is logged in to an ACD server has set his status as available.	Idle
barge	Barge	Allows another user to interrupt a shared call.	Shared-Active, Shared-Held
bxfer	BlindXfer/ bxfer	Performs a blind call transfer (transfers a call without speaking to the party to whom the call is transferred). Requires that Blind Xfer Serv is enabled.	Connected, Connected
cancel	Cancel	Cancels a call (for example, when conferencing a call and the second party is not answering).	Dialing Input

Keyword	Key Label	Definition	Available Phone States
cfwd	Forward	Forwards all calls to a specified number.	Idle, Off-Hook, Hold, Shared-Active, Shared-Held
chkcfwd	Clr Fwd/-cfwd	Deactivates call forwarding.	Idle
chkdnd	Clr DND/-dnd	Deactivates Do Not Disturb.	Idle
clear	Clear	Clears an entire text/number field.	Input
conf	Conf	Initiates a conference call. Requires that Conf Serv is enabled and there are two or more calls that are active or on hold.	Connected, Start-Conf
confLx	Conf Line	Conferences active lines on the phone. Requires that Conf Serv is enabled and there are two or more calls that are active or on hold.	Connected
delchar	delChar	Deletes a character when entering text.	Dialing (input)
dial	Dial	Dials a number.	Dialing (input)
dir	Dir	Provides access to phone directories.	Idle, Connected, Start-Conf, Start-Xfer, Off-Hook (no input), Redial
dnd	DND	Sets Do Not Disturb to prevent calls from ringing the phone.	Idle, Off-Hook (no input), Hold, Shared-Active, Shared-Held
em_login	Login	Logs user in to Extension Mobility.	Idle
em_logout	Logout	Logs user out of Extension Mobility.	Idle

Keyword	Key Label	Definition	Available Phone States
endcall	End Call	Ends a call.	Progressing, Start-Xfer, Start-Conf, Conferencing, Releasing, Resume
gpickup	GrPickup/ grPick	Allows user to answer a call ringing on an extension by discovering the number of the ringing extension.	Idle, Off-Hook (no input)
hold	Hold	Put a call on hold.	Connected, Start-Xfer, Start-Conf, Conferencing
ignore	Ignore	Ignores an incoming call.	Ringing
join	Join	Connects a conference call.	Conferencing
lcr	Call Rtn/lcr	Returns the last missed call.	Idle, Missed-Call, Off-Hook (no input)
left	Left	Moves the cursor to the left.	Dialing Input
miss	Miss	Displays the list of missed calls.	Missed-Call
newcall	New Call	Begins a new call.	Hold, Shared-Active
option	Option	Opens a menu of input options.	Off-Hook (no input), Dialing (input)
park	Park	Puts a call on hold at a designated “park” number.	Connected
phold	PrivHold	Puts a call on hold on an active shared line.	Connected
pickup	Pickup	Allows user to answer a call ringing on another extension by entering the extension number.	Idle, Off-Hook (no input)

Keyword	Key Label	Definition	Available Phone States
redial	Redial	Displays the redial list.	Idle, Connected, Start-Conf, Start-Xfer, Off-Hook (no input), Hold
resume	Resume	Resumes a call that is on hold.	Idle, Hold, Shared-Held
right	Right	Moves the cursor to the right.	Dialing (input)
starcode	Input Star Code/ *code	Displays a list of star codes that can be selected.	Off-Hook, Dialing (input)
toggle	Toggle	Switches between two calls that are active or on hold. (Cisco SPA 502)	Connected
unavail	Unavail	Denotes that a user who is logged in to an ACD server has set his status as unavailable.	Idle
unpark	Unpark	Resumes a parked call.	Idle, Off-Hook (no input)
xfer	Transfer/ xfer	Performs a call transfer. Requires that Attn Xfer Serv is enabled and there is at least one connected call and one idle call.	Connected, Start-Xfer
xferLx	Xfer Line/ xferLx	Transfers an active line on the phone to a called number. Requires that Attn Xfer Serv is enabled and there are two or more calls that are active or on hold.	Connected

Programmable Softkeys

The Cisco SPA 500 Series IP Phones provide six programmable softkeys (fields PSK 1 through PSK 6). These keys can be defined by either a speed dial script or an XML service script.

To configure programmable softkeys:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 In the Programmable Softkeys section, under Programmable Softkey Enable, choose **yes**.

To configure a speed dial script, enter the following in the PSK field:

fnc=sd;ext=*extensionname*@$PROXY;vid=*outboundextnum*;nme=*name*

where *fnc* is the function of the key (speed dial), ext (*extensionname*) is the extension being dialed, *vid* is the extension on the calling phone from which the outbound call is sent, and *name* is the name of the speed dial being configured.

NOTE The *name* field displays on the softkey on the phone display screen. Cisco recommends a maximum of 8 characters for a Cisco SPA 50X phone and 10 characters for a Cisco SPA 525G phone. If more characters are used, the label can be truncated on the phone display.

To configure an XML script, enter the following in the PSK field:

fnc=xml;url=http://*scriptURL.xml*;nme=*scriptname*

where *fnc* is the function of the key (an XML script), *scriptURL.xml* is the URL where the script is located, and *scriptname* is the name of the script.

NOTE The *scriptname* field displays on the softkey on the phone display screen. Cisco recommends a maximum of 8 characters for a Cisco SPA 50X phone and 10 characters for a Cisco SPA 525G phone. If more characters are used, the label can be truncated on the phone display.

You can use macro variables in XML URLs. The following macro variables are supported:

- User ID—UID1, UID2
- Display name—DISPLAYNAME1, DISPLAYNAME2

- Auth ID—AUTHID1, AUTHID2
- Proxy—PROXY1, PROXY2
- MAC Address—MA
- Product Name—PN
- Product Series Number—PSN
- Serial Number—SERIAL_NUMBER

STEP 5 Click **Submit All Changes**.

Configuration Example

You want to configure the Cisco SPA 525G phone with softkey that, when pressed, dials the Sales Department's extension (200). You want this button to display on the far lower left of the screen when the phone is idle, when the phone is off hook, or when the phone is connected on a call. You want the outbound call (that is going to the speed dial) to originate from the second extension on the user's phone, not the primary extension.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 In the Programmable Softkeys section, edit the following:

- Programmable Softkey Enable: yes
- PSK1: fnc=sd;ext=200@$PROXY;vid=2;nme=Sales
- Idle Key List: Edit the field to add psk1|1 to the beginning of the string; for example:

  ```
  psk1|1;em_login;acd_login;acd_logout;avail;unavail;
  redial;dir;cfwd;dnd;lcr;pickup;gpickup;unpark;em_logout;
  ```

- Off Hook Key List: Edit the field to add psk1|1 to the beginning of the string; for example:

  ```
  psk1|1;option;redial;dir;cfwd;dnd;lcr;unpark;pickup;
  gpickup;
  ```

- Connected Key List: Edit the field to add psk1|1 to the string, editing the existing *softkeyname*1 to PSK1. For example, the original string:

  ```
  hold|1;endcall|2;conf|3;xfer|4;bxfer;confLx;xferLx;park;p
  hold;flash;
  ```

  becomes:

  ```
  psk|1;hold|2;endcall|3;conf|4;xfer;bxfer;confLx;xferLx;
  park;phold;flash
  ```

STEP 5 Click **Submit All Changes**. The "Sales" speed dial softkey is displayed in the lower left of the screen when the phone is idle, when the phone is connected on a call, and when the phone is off hook.

Configuring the Message Waiting Indicator

You can configure the message waiting indicator (MWI) for separate extensions on the phone. The MWI lights based on the presence of new voicemail messages in the mailbox. However, if the indicator at the top of your Cisco SPA 500 Series IP Phone is not lighting when voice mail is left, or you are not seeing message waiting notifications on your WIP310:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Ext** <number> tab.

STEP 4 Under **Call Feature Settings**, in the **Message Waiting** field, choose **yes**.

STEP 5 Click **Submit All Changes**.

Configuring Ring Tones

You can define up to ten ring tones for a Cisco SPA 500 Series IP Phone.

NOTE WIP310 ring tones are not configurable from the web administration interface.

You can define:

- The default ring tone for the extension
- Specific ring tones assigned to individual callers in the personal directory. These override the default ring tone.

To configure ring tones:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab and proceed to the **Ring Tone** section.

You can configure the characteristics of each ring tone using a Ring Tone script. In a Ring Tone script, you can assign a name for the ring tone, and specify:

- Name (n)—Ring tone name, such as Classic, Simple, and Office
- Waveform (w)—1, 2, 3, or 4
- Cadence (c)—1, 2, 3, 4, or 5

You can also download one of two available ring tones (user ring tone 1 or 2) using TFTP:

`http://phone_ip_addr/ringtone1?[url]`

- Where the URL syntax is tftp:*//host[:port]/path*.
- The default host is the TFTP host.
- Port is optional. The default port is 69.
- The link is case sensitive.

On the IP phones, user-downloaded ring tones are labeled User 1 and User 2 in the choices for the Default Ring. On the phone ring tone menu, the User 1 and 2 choices are replaced by the corresponding name of the ring tone. “Not Installed” appears if the user ring tone slots are not used.

For ring tone User 1 and User2, the cadence is fixed with the on-time equals to the duration of the ring tone file and off-time equals to four seconds. The total ring duration is fixed at 60 seconds. The user ring tone names displayed on the phone LCD are derived from the ring tone file header file.

The phone does not require rebooting after downloading a ring tone.

To remove the User 1 ring tone from the phone, set the *path* to delete, as follows:

`http://phone_ip_addr/ringtone1?/delete`

STEP 4 Click **Submit All Changes**.

Configuring On-Demand Ring Tones (Cisco SPA 525G)

The Cisco SPA 525G supports on-demand ring tones, which means that ring tones are downloaded and played from a TFTP server when a call comes in. To configure:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Ring Tone**, in one or more of the ten ring tone fields, enter the following:

```
n=office;w=[tftp://]host[:port]/path;c=0
```

and specify the URL to download in the host/port/path field. If the connection cannot be established, a default ring tone is played.

STEP 5 Click **Submit All Changes**.

User-Created MP3 Ring Tones (Cisco SPA 525G)

Cisco SPA 525G users can create up to two ring tones from an MP3 audio file stored on a USB memory device. For instructions, see the *Cisco Small Business Pro SPA 525G User Guide (SIP)*, located on Cisco.com. (See **Appendix C, "Where to Go From Here,"** for the location of this document.)

Creating and Uploading Ring Tones Using the Ring Tone Utility (Cisco SPA 50XG only)

To convert a file for use as a ring tone, use the Ring Tone Utility, available at:

https://www.myciscocommunity.com/docs/DOC-6672

You must have a wav file less than 8 seconds in length saved to your computer. You can also use a sound editor to create the file with the following restrictions:

- 16-bit PCM mono
- 8000 samples per second
- less than 6000 ms in length

To create a ring tone and upload it to a phone:

STEP 1 Open the Ring Tone Utility.

STEP 2 Enter the IP address of the phone.

STEP 3 Click **Browse** and navigate to the directory on your computer where the source .wav file is stored. Select the wav file and click **Open**.

STEP 4 Click **Load Source File**.

STEP 5 Enter a name for the ring tone. This name will appear in the display on the phone. You choose the file name later.

STEP 6 Enter the target. You can have up to two customized ring tones uploaded to the phone.

STEP 7 (Optional) Click **Preview** to preview the ring tone. Click **Options** to change the start or end positions, or to squeeze or stretch the audio.

STEP 8 Click **Upload to Phone** to upload the ring tone to the phone. Click **OK** when the success status message appears.

STEP 9 Close the open Ring Tone Utility windows.

To create a ring tone and save it to a file:

STEP 1 Open the Ring Tone Utility.

STEP 2 Enter the IP address of the user's phone or press **Skip** to create the ring tone and save it as a file.

STEP 3 Click **Browse** and navigate to the directory on your computer where the source wav file is stored. Select the wav file and click **Open**.

STEP 4 Click **Load**.

STEP 5 Enter a name for the ring tone. This name will appear in the phone display. You choose the file name later.

STEP 6 (Optional) Click **Preview** to preview the ring tone. Click **Options** to change the start or end positions, or to squeeze or stretch the audio.

STEP 7 Click **Save As** to save the file to your computer. Enter the file name and press **Save**.

STEP 8 Close the open Ring Tone Utility windows.

To delete a ring tone from a phone:

STEP 1 Open the Ring Tone Utility.

STEP 2 Enter the IP address of the phone.

STEP 3 Click the **Delete** button next to the ring tone you want to delete.

STEP 4 Click **OK**.

STEP 5 Close the open Ring Tone Utility windows.

Assigning a Ring Tone to an Extension

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Ext** <number> tab.

STEP 4 Under **Call Feature Settings**, in the **Default Ring** field, choose from the following:

- No Ring
- 1 through 10
- User 1
- User 2

STEP 5 Click **Submit All Changes**.

Configuring RSS Newsfeeds on the Cisco SPA 525G IP Phone

The Cisco SPA 525G provides the option to view RSS newsfeeds for news in the categories of local, world, finance, sports, and politics. Newsfeeds that are provided by Yahoo are supported for U.S. customers only.

To configure newsfeeds:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Web Information Service Settings**, you can edit the following fields:

Parameter	Description
RSS Feed URLs 1-5	URLs for Local and World news, Finance, Sports, and Politics. Default values are: ▪ 1—Local News (defaults to URL http://rss.cnn.com/rss/cnn_us.rss) ▪ 2—World News (defaults to URL http://newsrss.bbc.co.uk/rss/newsonline_uk_edition/world/rss.xml) ▪ 3—Finance News (defaults to URL http://finance.yahoo.com/rss/topstories) ▪ 4—Sports News (defaults to URL http://rss.news.yahoo.com/rss/sports ▪ 5—Politics News (defaults to URL http://rss.news.yahoo.com/rss/politics)
Weather Temperature Unit	Choose which unit to display for weather information (Fahrenheit or Celsius).

STEP 5 Click **Submit All Changes**. The phone reboots.

Configuring Audio Settings

You can configure default audio volume settings for the phone. These settings can be modified by the user by pressing the volume control button on the phone, then pressing the **Save** soft button. (Not applicable to the WIP310.)

To configure the audio volume settings:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab. You can configure the following settings:

Parameter	Description
Ringer Volume	Sets the volume for the ringer.
Speaker Volume	Sets the volume for the full-duplex speakerphone.
Handset Volume	Sets the volume for the handset.
Headset Volume	Sets the volume for the headset.
Bluetooth Volume	Sets the volume for the Bluetooth device. **NOTE** Applies to Cisco SPA 525G only.

STEP 4 Click **Submit All Changes**.

Configuring Audio Input Gain (Cisco SPA 500 Series)

You can amplify or deamplify the sound on your phone's handset, headset, and speakerphone.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under Audio Input Gain (dB), choose the item to configure.

- If you enter a positive value, amplification increases (sound is louder).
- If you enter a negative value, amplification decreases (sound is softer).
- You can enter a value from -6 decibels to +6 decibels. All fields default to zero.

- Try a value that is loud enough without producing echo (an issue if the input gain is too high).

STEP 5 Click **Submit All Changes**.

Enabling Wireless (Cisco SPA 525G only)

The Cisco SPA 525G provides a built-in Wireless-G interface. To enable wireless:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Under **Wi-Fi Settings**, in the **SPA525-wifi-on** field, choose **yes**.

STEP 5 Click **Submit All Changes**.

Enabling Bluetooth (Cisco SPA 525G only)

The Cisco SPA 525G supports Bluetooth to allow use of the phone with a wireless Bluetooth-enabled headset. To enable Bluetooth:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Under **Bluetooth Settings**, in the **Enable BT** field, choose **yes**.

STEP 5 Click **Submit All Changes**.

Enabling SMS Messaging

These Cisco IP phones can receive and display text messages via SIP according to RFC3428. Users can receive text messages. WIP310 users can send *and* receive text messages.

When this feature is enabled, the phone displays messages up to 255 characters in length. The message appears on the phone display along with the date and time.

Service providers could use text messages to:

- Send billing information, calling minutes consumed, minutes available
- Include additional text with a call to facilitate call processing

Cisco SPA 50XG:

To enable text message receipt on the Cisco SPA 50XG phones:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Supplementary Services**, in the **Text Message** field, choose **yes**.

STEP 5 (Optional) To enable receipt of text messages from a third party directly without proxy involvement, in the **Text Message from 3rd Party** field, choose **yes**.

STEP 6 Click **Submit All Changes**.

Cisco SPA 525G

To enable text messaging on the Cisco SPA 525G phones:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **User** tab.

STEP 4 Under **Supplementary Services**, in the **Display Text Message on Recv** field, choose **yes**.

STEP 5 (Optional) To enable receipt of text messages from a third party directly without proxy involvement, in the **Text Message from 3rd Party** field, choose **yes**.

STEP 6 Click **Submit All Changes**.

WIP310

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **SMS Enable**, choose **yes**.

STEP 5 Click **Submit All Changes**.

Enabling the Web Server

The web server allows administrators and users to log in to the phone using a web interface. Administrators and users have different privileges and see different options for the phone based on their role.

To enable the web server:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 In the **Enable Web Server** field, choose **yes** to enable the web administration server for the phone. (For the Cisco SPA 501G, can be configured using the IVR. See the **"Using IVR on the Cisco SPA 501G IP Phone" section on page 17**.)

STEP 5 In the **Web Server Port** field, enter the port to access the server. The default is port 80 for the web UI.

STEP 6 In the **Enable Web Admin Access** field, you can enable or disable local access to the **Admin Login** of the web UI. Defaults to **yes** (enabled). (For the Cisco SPA 501G,

can be configured using the IVR. See the **"Using IVR on the Cisco SPA 501G IP Phone" section on page 17**.)

STEP 7 In the **Admin Passwd** field, enter a password if you want the system administrator to log on to the web UI with a password. The password prompt will appear when an administrator clicks **Admin Login**. The maximum password length is 32 characters.

STEP 8 In the **User Password** field, enter a password if you want users to log on to the web UI with a password. The password prompt will appear users click **User Login**. The maximum password length is 32 characters

STEP 9 Click **Submit All Changes**.

You can also enable the web administration interface from the **Phone** tab (does not apply to the WIP310):

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Web Serv**, choose **yes**.

STEP 5 Click **Submit All Changes**.

Configuring Lightweight Directory Access Protocol (LDAP) for the Cisco SPA 500 Series

The Cisco SPA 500 Series IP Phones support Lightweight Directory Access Protocol v3 to enable the retrieval of directory information. The LDAP Corporate Directory Search feature, when configured and enabled on a Cisco SPA 500 Series IP Phone, allows a user to search a specified LDAP directory for a name, phone number, or both. (LDAP is not supported on the WIP310.)

LDAP-based directories, such as Microsoft Active Directory 2003 and OpenLDAP-based databases, are supported.

These instructions assume you have the following equipment and services:

- A functional LDAP server such as OpenLDAP or Microsoft's Active Directory Server 2003
- A Cisco SPA 500 Series IP Phone running at least 6.1.3a software on a functional network

Users access LDAP from the **Directory** menu on their IP phone. There is a limit of 20 records returned from an LDAP search.

Before you use the LDAP Corporate Directory Search feature of your phone, you need to configure some basic information.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 In the **Optional Network Configuration** section, under **Primary DNS**, enter the IP address of the DNS server. (Only required if using Active Directory with authentication set to MD5.)

STEP 5 In the **Optional Network Configuration** section, under **Domain**, enter the LDAP domain. (Only required if using Active Directory with authentication set to MD5.)

NOTE Some sites may not deploy DNS internally and instead use Active Directory 2003. In this case, it is not necessary to enter a Primary DNS address and an LDAP Domain. However, with Active Directory 2003, the authentication method is restricted to Simple.

STEP 6 Click the **Phone** tab.

STEP 7 Under **LDAP Corporate Directory Search**, in the **LDAP Dir Enable** field, choose **yes** to enable LDAP and cause the name defined in **LDAP Corp Dir Name** to appear in the phone's Directory menu.

STEP 8 Configure values for the fields in the following table and click **Submit All Changes**.

Parameter	Description
LDAP Corp Dir Name	Enter a free-form text name, such as “Corporate Directory.”
LDAP Server	Enter a fully qualified domain name or IP address of LDAP server, in the following format: `nnn.nnn.nnn.nnn` Enter the host name of the LDAP server if the MD5 authentication method is used.
LDAP Auth Method	Select the authentication method that the LDAP server requires. Choices are: ▪ None—No authentication is used between the client and the server. ▪ Simple—The client sends its fully-qualified domain name and password to the LDAP server. May present security issues. ▪ Digest-MD5—The LDAP server sends authentication options and a token to the client. The client returns an encrypted response that is decrypted and verified by the server.

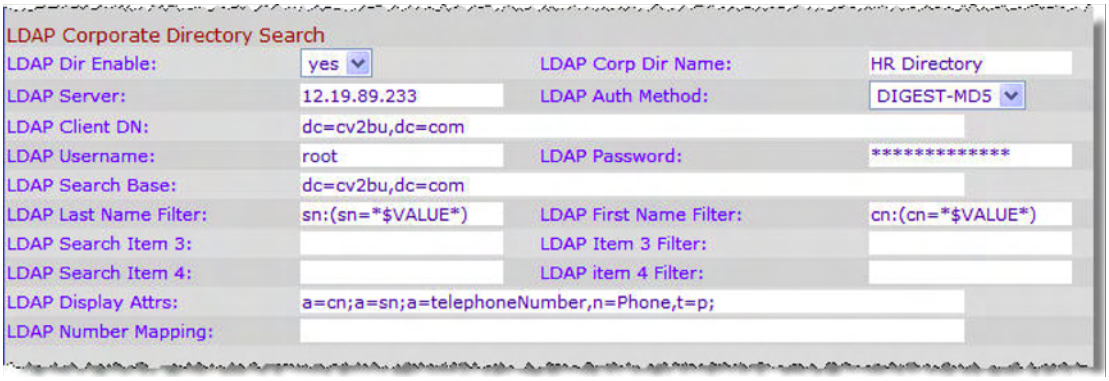
LDAP Client DN	Enter the distinguished name domain components [dc] ; for example:
	`dc=cv2bu,dc=com`
	If using the default Active Directory schema (Name(cn)->Users->Domain), an example of the client DN follows:
	`cn="David Lee",dc=users,dc=cv2bu,dc=com`

LDAP Username	Enter the username for a credentialed user on the LDAP server.
LDAP Password	Enter the password for the LDAP username.
LDAP Search Base	Specify a starting point in the directory tree from which to search. Separate domain components [dc] with a comma. For example: dc=cv2bu,dc=com

Parameter	Description
LDAP Last Name Filter	This defines the search for surnames [sn], known as last name in some parts of the world. For example, sn:(sn=*$VALUE*). This search allows the provided text to appear anywhere in a name, beginning, middle, or end. You must enter a value in both the last name and first name fields so that the LDAP corporate directory option displays on the phone. If both fields are empty, the directory does not display.
LDAP First Name Filter	This defines the search for the common name [cn]. For example, cn:(cn=*$VALUE*). This search allows the provided text to appear anywhere in a name, beginning, middle, or end. You must enter a value in both the last name and first name fields so that the LDAP corporate directory option displays on the phone. If both fields are empty, the directory does not display.
LDAP Search Item 3	Additional customized search item. Can be blank if not needed.
LDAP Item 3 Filter	Customized filter for the searched item. Can be blank if not needed.
LDAP Search Item 4	Additional customized search item. Can be blank if not needed.
LDAP Item 4 Filter	Customized filter for the searched item. Can be blank if not needed.
LDAP Display Attrs	Format of LDAP results display on phone where: ▪ a—Attribute name (such as cn, sn, and telephoneNumber) ▪ n—Display name ▪ t—type ▪ p—phone number For example: `a=cn, n=Name;a=telephoneNumber,n=Phone,t=p;`

Parameter	Description
LDAP Number Mapping	Can be blank if not needed. Uses the same syntax as the “dial plan” field. **NOTE** With the LDAP number mapping you can manipulate the number that was retrieved from the LDAP server. For example, you can append 9 to the number if your dial plan requires a user to enter 9 before dialing. If you do not manipulate the number in this fashion, a user can use the **Edit Dial** feature to edit the number before dialing out.

The following graphic is an example of an LDAP configuration:



For more information on LDAP, including troubleshooting information, see the *Configuring LDAP Directory Search on SPA SIP IP Phones* Application Note, available from http://www.cisco.com/web/partners/sell/smb/products/voice_and_conferencing.html#~vc_technical_resources (partner log on required).

Configuring BroadSoft Settings (Cisco SPA 500 Series)

Configuring BroadSoft Directory

The BroadSoft directory service enables users to search and view their personal, group, or enterprise contacts. This application feature uses BroadSoft's Extended Services Interface (XSI).

To configure the BroadSoft Directory service:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Broadsoft Settings**, configure the following:

- Directory Enable: Set to **yes**.
- XSI Host Server: Enter the name of the server; for example, xsp.xdp.broadsoft.com.
- Directory Name: Name of the directory. Displays on the user's phone as a directory choice (for example, "John's Personal Directory").
- Directory Type: Select the type of BroadSoft directory:
  - Enterprise (default): Allows users to search on last name, first name, user or group ID, phone number, extension, department, or email address.
  - Group: Allows users to search on last name, first name, user ID, phone number, extension, department, or email address.
  - Personal: Allows users to search on last name, first name, or telephone number.
- Directory UserID: BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com.
- Directory Password: Alphanumeric password associated with the User ID.

STEP 5 Click **Submit All Changes**.

Configuring Synchronization of Do Not Disturb and Call Forward

Enabling synchronization of Do Not Disturb and Call Forward allows the phone to synchronize with the call server (for example, the BroadSoft server) so that if Do Not Disturb or Call Forwarding settings are changed on the phone, changes are also made on the server; if changes are made on the server, they are propagated to the phone.

This feature is disabled by default.

To enable synchronization:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Broadsoft Settings**, in the **Call Feature Sync Ext** field, choose the extension (1 through 5) that is registered to the BroadSoft server.

STEP 5 Click **Submit All Changes**.

Configuring XML Services

The Cisco SPA 500 Series IP Phones provide support for XML services, such as an XML Directory Service or other XML applications.

The following table shows some Cisco XML objects that are supported by the Cisco SPA 500 Series IP Phones:

Cisco XML Object	Supported Phone
CiscoIPPhoneMenu	Cisco SPA 525G, Cisco SPA 50X
CiscoIPPhoneText	
CiscoIPPhoneInput	
CiscoIPPhoneDirectory	
CiscoIPPhoneImage	Cisco SPA 525G
CiscoIPPhoneImageFile	
CiscoIPPhoneGraphicMenu	
CiscoIPPhoneIconMenu	Cisco SPA 525G, Cisco SPA 50X

Cisco XML Object	Supported Phone
CiscoIPPhoneFileMenu	Cisco SPA 525G
CiscoIPPhoneStatus	
CiscoIPPhoneStatusFile	
CiscoIPPhoneExecute	Cisco SPA 525G, Cisco SPA 50X
CiscoIPPhoneResponse	Cisco SPA 525G
CiscoIPPhoneErrror	
CiscoIPPhoneGraphicFileMenu	

You can use macro variables in XML URLs. The following macro variables are supported:

- User ID—UID1, UID2
- Display name—DISPLAYNAME1, DISPLAYNAME2
- Auth ID—AUTHID1, AUTHID2
- Proxy—PROXY1, PROXY2
- MAC Address—MA
- Product Name—PN
- Product Series Number—PSN
- Serial Number—SERIAL_NUMBER

For more information on XML support, see the Cisco Small Business Support community. The URL is given in **Appendix C, "Where to Go From Here."**

To configure the phone to connect to an XML Directory service:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Enter the following information:

- XML Directory Service Name: Name of the XML Directory. Displays on the user's phone as a directory choice.
- XML Directory Service URL: URL where the XML Directory is located.

STEP 5 Click **Submit All Changes**.

To configure the phone to connect to an XML application:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Enter the following information:

- XML Application Service Name: Name of the XML application. Displays on the user's phone as a menu item.
- XML Application Service URL: URL where the XML application is located.

NOTE If you have configured an unused line button to connect to an XML application, the button connects to the URL configured here, unless you enter a different URL when configuring the line button. See the **"Configuring Unused Line Keys to Access Services" section on page 27**.

STEP 5 Click **Submit All Changes**.

Configuring Music On Hold

Your phone can play music on hold if it is part of a system that has a music-on-hold (MOH) server. To configure music on hold:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Ext** <number> tab.

STEP 4 Under **Call Feature Settings**, in the **MOH Server** field, enter the user ID or the URL of the MOH streaming audio server. If you enter a user ID (no server), the current or outbound proxy is contacted. Defaults to blank (no MOH). If used with a Cisco SPA 9000 Voice System, defaults to *imusic*. For more information, see the *Cisco SPA 9000 Voice System Administration Guide*.

STEP 5 Click **Submit All Changes**.

Configuring Extension Mobility with a BroadSoft Server

NOTE This feature is not available on the WIP310.

If your phones use a BroadSoft server, users can dynamically log in on their phones using extension mobility (EM).

EM lets people who work different shifts or who work at different desks during the week share an extension. EM dynamically configures a phone according to the current user. A Login prompt appears on the phone display when EM is enabled. The user must enter their User ID and Password.

For example, when User A logs in to the phone, all of her personal phone settings are available. Later in the day, User B can log in to the same phone and use his personal settings. After logging on, users have access to personal directory numbers, services, speed dials, and other properties on their phone.

When a user logs out, the phone reverts to a basic profile with limited features enabled.

To configure extension mobility:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 Under **Extension Mobility**, in the **EM Enable** field, choose **yes**.

STEP 5 In the **EM User Domain** field, enter the BroadSoft domain for the phone.

STEP 6 Click **Submit All Changes**. The phone reboots.

You must also configure the Extension Mobility parameters in the profile rule field in the Provisioning tab. See the *Provisioning Parameters for Extension Mobility on Cisco SPA500 Series IP Phones* application note at:

https://www.myciscocommunity.com/docs/DOC-11277

For more information on extension mobility and BroadSoft, see http://www.broadsoft.com.

Configuring Video Surveillance on the Cisco SPA 525G

The Cisco SPA 525G provides a simple video surveillance solution for a small business office. The Cisco SPA 525G works with the Cisco WVC2300 Wireless-G Business Internet Video Camera and the Cisco PVC2300 Business Internet Video Camera to provide simple video monitoring from your IP phone of a location such as a lobby entrance or doorway. Up to four cameras can be monitored from one IP phone.

NOTE Camera audio is not supported.

The Cisco SPA 525G connects to the videocamera and provides a real-time video stream display from the camera. Storage and manipulation of video and physical camera control are not available from the IP phone.

The IP phone supports the camera display at a rate of two to three frames per second with good video quality. However, video quality can degrade if the camera is processing multiple streaming sessions, there is heavy Wi-Fi network traffic, or the IP phone is performing other processing. To avoid degrading voice audio quality on a call, the frame rate decreases to one frame per second if a codec other than G.711 is used for a call or when the user accesses the video monitoring page during a call.

To configure the video surveillance feature, perform the steps outlined in the following sections.

Configuring the User Name and Account on the Camera

STEP 1 Download and install the software release for the camera that provides video monitoring support. For more information, consult the release notes for the camera software.

STEP 2 After installing the camera software, use the administration interface to create a user ID and password that will be used by the phone to connect to the camera. The IP phone user account that you create should have viewer privileges.

Entering Camera Information Into the Cisco SPA525G Web Administration Interface

STEP 1 Log in to the web administration interface.

STEP 2 Click the **User** tab.

STEP 3 Under Camera Settings, in the Enable Video VLAN field, choose yes. This option separates camera traffic to a separate VLAN.

STEP 4 (Optional) If configuring Virtual LAN (VLAN) support, in the Enable Video VLAN field, choose **yes**. The default Video VLAN ID is 1, the data VLAN. To separate traffic onto another VLAN (for example, a VLAN for video traffic only), enter the ID for that VLAN. (Video VLAN parameters do not apply to Wi-Fi or VPN.)

STEP 5 Under Camera Profile 1, enter the settings for the first camera. Enter the camera name (for example, **Lobby**). This name is displayed on the phone display screen to identify the camera.

STEP 6 In the Access URL field, enter the URL to access the camera, in the following format:

```
rtsp://xxx.xxx.x.xxx/img/jpgvideo.sav
```

where *xxx.xxx.x.xxx* is the IP address of the camera.

STEP 7 In the Access User Name field, enter the username for the phone that you created using the camera's administration interface.

STEP 8 In the Access Password field, enter the password for the phone username that you created using the camera's administration interface.

STEP 9 (Optional) In the Associated Caller ID field, enter the phone number of the phone associated with the camera. For example, if the camera is located in the lobby, you may want to enter the extension of the lobby phone if one is installed there. People monitoring that camera from their phone can press **Call** to dial the number of the phone associated with the camera. For example, someone monitoring the lobby could call the receptionist to identify a visitor.

STEP 10 Repeat Step 4 through Step 8 for each camera.

STEP 11 Click **Submit All Changes**.

Viewing the Video

To view video from the phone:

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Video Monitoring** and press **Select**.

STEP 3 Scroll to the camera from which you want to view and press **Monitor** or **Select**.

Pressing Call dials the number associated with the camera (see **Entering Camera Information Into the Cisco SPA525G Web Administration Interface, page 78**).

4

Configuring SIP, SPCP, and NAT

The Cisco SPA 500 Series and Wireless IP Phones use the following protocols:

- Session Initiation Protocol (SIP)—Cisco SPA 500 Series, WIP310
- Cisco Smart Phone Control Protocol (SPCP)—Cisco SPA 500 Series

This chapter describes how to configure the phone protocols and other parameters. It contains the following sections:

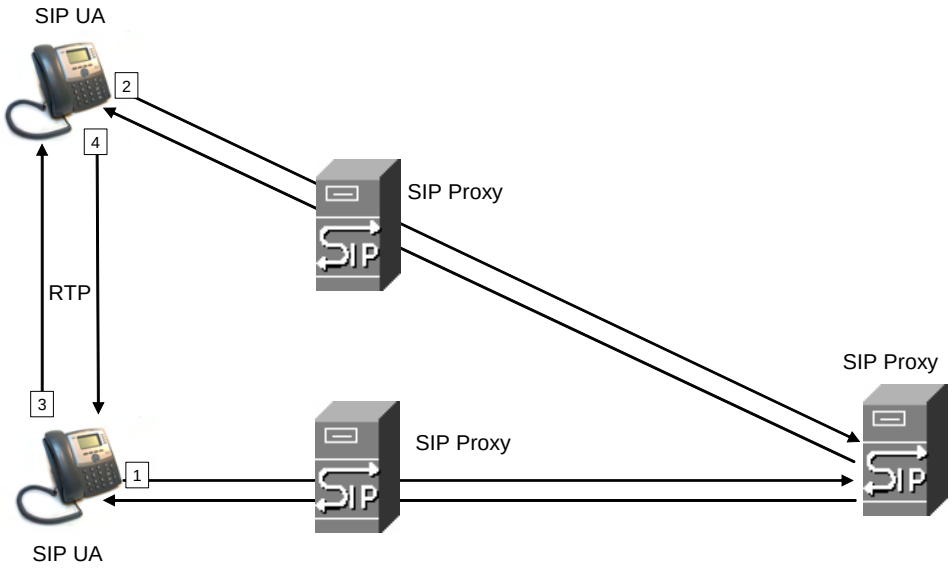
Session Initiation Protocol and Cisco IP Phones

Cisco IP phones use Session Initiation Protocol (SIP), allowing interoperation with all ITSPs supporting SIP.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

The following diagram shows a SIP request for connection to another subscriber in the network.

In typical commercial IP telephony deployments, all calls go through a SIP proxy server. The requesting phone is called the SIP user agent server (UAS), while the receiving phone is called the user agent client (UAC).



SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response is routed back to the UAS, and a direct peer-to-peer session is established between the two UAs. Voice traffic is transmitted between UAs over dynamically-assigned ports using Real-time Protocol (RTP).

The Internet protocol RTP transmits real-time data such as audio and video; it does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of the UDP protocol. See **"Configuring NAT Mapping with STUN" section on page 106**.

SIP Over TCP

To guarantee state-oriented communications, Cisco IP phones can use TCP as the transport protocol for SIP. This protocol is "guaranteed delivery", which assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

TCP overcomes the problem with UDP ports being blocked by corporate firewalls. With TCP, new ports do not need to be opened or packets dropped, because TCP is already in use for basic activities such as Internet browsing or e-commerce.

SIP Proxy Redundancy

An average SIP proxy server may handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. Cisco phones support the use of backup SIP proxy servers to minimize or eliminate service disruption.

A static list of proxy servers is not always adequate. If your user agents are served by different domains, for example, you would not want to configure a static list of proxy servers for each domain into every Cisco IP phone.

A simple way to support proxy redundancy is to configure a SIP proxy server in the Cisco IP phone configuration profile. The DNS SRV records instruct the phones to contact a SIP proxy server in a domain named in SIP messages. The phone consults the DNS server. If configured, the DNS server returns an SRV record that contains a list of SIP proxy servers for the domain, with their host names, priority, listening ports, and so on. The Cisco IP phone tries to contact the hosts in the order of their priority.

If the Cisco IP phone currently uses a lower-priority proxy server, the phone periodically probes the higher-priority proxy and switches to the higher-priority proxy when available.

Configuring Survivable Remote Site Telephony (SRST) Support

The *proxy* and *outbound proxy* fields in the **Ext** tab can be configured with an extension that includes a statically-configured DNS SRV record or DNS A record. This allows for failover and fallback functionality with a secondary proxy server. The format for the parameter value is as follows:

```
FQDN format: hostname[:port][:SRV=host-list OR :A=ip-list]
host-list:  srv[|srv[|srv…]]
srv: hostname[:port][:p=priority][:weight][:A=ip-list]
ip-list: ip-addr[,ip-addr[,ip-addr…]]
```

The default priority is 0 and default weight is 1. The default port is 0, and the application substitutes the proper port value (for example, port 5060 for SIP).

RFC3311 Support

The Cisco SPA 525G supports RFC3311, the SIP UPDATE Method.

Support for SIP NOTIFY XML-Service

The Cisco SPA 500 Series IP Phones support the SIP NOTIFY XML-Service event. On receipt of a SIP NOTIFY message with an XML-Service event, the IP phone challenges the NOTIFY with a 401 response if the message does not contain correct credentials. The client must be furnish the correct credentials using MD5 digest with the SIP account password for the corresponding line of the IP phone.

The body of the message may contain the XML event Message. For example:

```
<CiscoIPPhoneExecute>
  <ExecuteItem Priority="0" URL="http://xmlserver.com/event.xml"/>
</CiscoIPPhoneExecute>
```

Authentication:

```
challenge  = MD5( MD5(A1) ":" nonce ":" nc-value ":" cnonce ":" qop-value
":" MD5(A2) )
where A1 = username ":" realm ":" passwd
and A2 = Method ":" digest-uri
```

Configuring SIP

SIP settings for the Cisco SPA 500 Series and Wireless IP Phones are configured for the phone in general and for individual extensions. The following sections describe SIP configuration.

Configuring SIP Parameters

To configure general SIP parameters, including enabling CTI:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **SIP** tab.

STEP 4 Under **SIP Parameters**, make the necessary configuration changes to the fields shown in the following table and click **Submit All Changes**.

Parameter	Description
SIP Reg User Agent Name	User-Agent name used in a REGISTER request. If not specified, the SIP User Agent Name is also used for the REGISTER request. Defaults to blank.
SIP Accept Language	Accept-Language header used. If empty, the header is not included. Defaults to blank.
DTMF Relay MIME Type	MIME Type used in a SIP INFO message to signal a DTMF event. This parameter must match that of the service provider. Defaults to application/dtmf-relay.
Remove Last Reg	If set to yes, removes the last registration before re-registering (if the value is different). Defaults to no.
Use Compact Header	If set to yes, the Cisco IP phone uses compact SIP headers in outbound SIP messages. If inbound SIP requests contain normal (non-compact) headers, the phone substitutes incoming headers with compact headers. If set to no, the Cisco IP phone uses normal SIP headers. If inbound SIP requests contain compact headers, the phone reuses the same compact headers when generating the response, regardless of this setting. Defaults to no.
Escape Display Name	Setting this parameter to yes encloses the configured Display Name string in a pair of double quotes for outbound SIP messages. Any occurrences of or \ in the string is escaped with \ and \\ inside the pair of double quotes. Defaults to yes.
SIP-B Enable	If set to yes, enables BroadSoft call features. See www.broadsoft.com for more information. Defaults to no.
Talk Package	If set to yes enables support for the BroadSoft Talk Package, which lets users answer or resume a call by clicking a button in an external application. Defaults to no.
Hold Package	If set to yes, enables support for the BroadSoft Hold Package, which lets users place a call on hold by clicking a button in an external application. Defaults to no.

Parameter	Description
Conference Package	If set to yes, enables support for the BroadSoft Conference Package, which enables users to start a conference call by clicking a button in an external application. Defaults to no.
Notify Conference	If set to yes, the Cisco IP phone sends out a NOTIFY with event=conference when starting a conference call (with the BroadSoft Conference Package). Defaults to no.
RFC 2543 Call Hold	If set to yes, the Cisco IP phone includes SDP syntax c=0.0.0.0 when sending a SIP re-INVITE to a peer to hold the call. If set to no, the Cisco IP phone does not include the c=0.0.0.0 syntax in the SDP. With either setting, the phone includes a=sendonly syntax in the SDP. Defaults to yes.
Random REG CID On Reboot	If set to yes, the IP phone uses a different random call-ID for registration after the next software reboot. If set to no, the IP phone tries to use the same call-ID for registration after the next software reboot. With either setting the phone uses a new random call-ID for registration after a power-cycle. Defaults to no. **NOTE** Not applicable to the WIP310.
Mark All AVT packets	If set to yes, all audio video transport (AVT) tone packets (encoded for redundancy) have the marker bit set. If set to no, only the first packet has the marker bit set for each DTMF event. Defaults to yes.
SIP TCP Port Min	Specifies the lowest TCP port number that can be used for SIP sessions. Defaults to 5060.
SIP TCP Port Max	Specifies the highest TCP port number that can be used for SIP sessions. Defaults to 5080.

Parameter	Description
CTI Enable	If set to yes, enables the computer telephony integration (CTI), where a computer can act as a call center handling all sorts of incoming and outgoing communications., including phone calls, faxes, and text messages. The CTI interface allows a third-party application to control and monitor the state of a Cisco IP phone and, for example, initiate or answer a call by clicking a mouse on a PC, **NOTE** CTI must be enabled on the Cisco SPA 500 Series IP Phone for an attached Cisco SPA 500S to properly monitor the Cisco SPA 500 Series IP phone's line status. If setting up a Cisco SPA 500S, see **Chapter 9, "Configuring the Cisco SPA 500S Attendant Console."** Defaults to no.
Caller ID Header	Select where the IP phone gets its caller ID from: PAID-RPID-FROM P-ASSERTED-IDENTITY REMOTE-PARTY-ID FROM header Defaults to PAID-RPID-FROM. **NOTE** Not applicable to the WIP310.
SRTP Method	Selects the method to use for SRTP. Two choices are available: ▪ x-sipura—legacy SRPT method ▪ s-descriptor—new method compliant with RFC-3711 and RFC-4568 The default value is "x-sipura." **NOTE** Not applicable to WIP310.
Hold Target Before REFER	Controls whether to hold call leg with transfer target before sending REFER to the transferee when initiating a fully-attended call transfer (where the transfer target has answered). Default value is "no," where the call leg is not held. **NOTE** Not applicable to WIP310.

Configuring SIP Timer Values

To configure SIP timer values:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **SIP** tab.

STEP 4 Under **SIP Timer Values**, make the necessary configuration changes to the fields shown in the following table and click **Submit All Changes**.

Parameter	Description
SIP T1	RFC 3261 T1 value (RTT estimate). Ranges from 0 to 64 seconds. Defaults to .5 seconds.
SIP T2	RFC 3261 T2 value, which is the maximum retransmit interval for non-INVITE requests and INVITE responses. Ranges from 0 to 64 seconds. Defaults to 4 seconds.
SIP T4	RFC 3261 T4 value, which is the maximum duration a message remains in the network. Ranges from 0 to 64 seconds. Defaults to 5 seconds.
SIP Timer B	RFC 3261 INVITE transaction time-out value. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer F	RFC 3261 Non-INVITE transaction time-out value. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer H	RFC 3261 INVITE final response time-out value for ACK receipt. Ranges from 0 to 64 seconds. Defaults to 16 seconds.

Parameter	Description
SIP Timer D	FRC 3261 wait time for response retransmits. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer J	RFC 3261 Wait time for Non-INVITE request retransmits. Ranges from 0 to 64 seconds. Defaults to 16 seconds.
INVITE Expires	INVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 240 seconds.
ReINVITE Expires	ReINVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 30
Reg Min Expires	Minimum registration expiration time allowed from the proxy in the Expires header or as a Contact header parameter. If the proxy returns a value less than this setting, the minimum value is used. Defaults to 1 second.
Reg Max Expires	Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is greater than this setting, the maximum value is used. Defaults to 7200 seconds.
Reg Retry Intvl (see Note below)	Interval to wait before the Cisco IP phone retries registration after failing during the previous registration. Do not enter 0. Defaults to 30 seconds.
Reg Retry Long Intvl (see Note below)	When registration fails with a SIP response code that does not match the Retry Reg response status code (RSC) value (see next table), the Cisco IP phone waits for this length of time before retrying. If this interval is 0, the Cisco IP phone stops trying. This value should be much larger than the Reg Retry Intvl value. Defaults to 1200 seconds.

Parameter	Description
Reg Retry Random Delay	Random delay added to the Register Retry Intvl value when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the short timer. Defaults to 0, which disables this feature.
Reg Retry Long Random Delay	Random delay add ed to Register Retry Long Intvl value when retrying REGISTER after a failure. Minimum and maximum random delay to be added to the long timer. Random delay range (in seconds) to add to the Register Retry Long Intvl when retrying REGISTER after a failure. Defaults to 0, which disables this feature. **NOTE** Not applicable to WIP310.
Reg Retry Intvl Cap	Reg_Retry_Intvl_Cap—Maximum value of the exponential delay. The maximum value to cap the exponential backoff retry delay (which starts at the Register Retry Intvl and doubles every retry). Defaults to 0, which disables the exponential backoff feature (that is, the error retry interval is always at the Register Retry Intvl). If this feature is enabled, the Reg Retry Random Delay is added on top of the exponential backoff delay value. **NOTE** Not applicable to WIP310.
Sub Min Expires	The lower limit of the REGISTER (subscribe) expires value returned from the proxy server. Defaults to 10 seconds.
Sub Max Expires	The upper limit of the REGISTER (subscribe) min-expires value returned from the proxy server in the Min-Expires header. Defaults to 7200 seconds.
Sub Retry Intvl	The retry interval when the last Subscribe request fails. Defaults to 10 seconds.

NOTE Cisco IP phones can use a RETRY-AFTER value when received from a SIP proxy server that is too busy to process a request (503 Service Unavailable message). If the response message includes a RETRY-AFTER header, the phone waits for the

specified length of time before retrying to REGISTER again. If a RETRY-AFTER header is not present, the phone waits for the value specified in the Reg Retry Interval or the Reg Retry Long Interval parameter.

Configuring Response Status Code Handling

To configure response status code handling:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **SIP** tab.

STEP 4 Under **Response Status Code Handling**, configure the following:

- **SIT1 through SIT4 RSC**—SIP response status code for the appropriate Special Information Tone (SIT). For example, if you set the SIT1 RSC to 404, when the user makes a call and a failure code of 404 is returned, the SIT1 tone is played. Reorder or Busy Tone is played by default for all unsuccessful response status code for SIT 1 RSC through SIT 4 RSC. Defaults to blank.
- **Try Backup RSC**—SIP response code that retries a backup server for the current request. Defaults to blank.
- **Retry Reg RSC**—Interval the SPA9000 waits before re-trying registration after a failed registration. Defaults to blank.

STEP 5 Click **Submit All Changes**.

Configuring RTP Parameters

To configure individual RTP parameters:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **SIP** tab.

STEP 4 Under **RTP Parameters**, configure the following fields:

- **RTP Port Min**—Minimum port number for RTP transmission and reception. <RTP Port Min> and <RTP Port Max> should define a range that contains at least 10 even number ports (twice the number of lines); for example, 100 – 106. Defaults to 16384.
- **RTP Port Max**—Maximum port number for RTP transmission and reception. <RTP Port Min> and <RTP Port Max> should define a range that contains at least 10 even number ports (twice the number of lines); for example, 100 – 106. Defaults to 16482.
- **RTP Packet Size**—Packet size in seconds, which can range from 0.01 to 0.16. Valid values must be a multiple of 0.01 seconds. Defaults to 0.030.
- **Max RTP ICMP Err**—Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the Cisco IP phone terminates the call. If the value is set to 0 (the default), the Cisco IP phone ignores the limit on ICMP errors, disabling the feature.
- **RTCP Tx Interval**—Interval for sending out RTCP sender reports on an active connection. During an active connection, the Cisco IP phone can be programmed to send out compound RTCP packet on the connection. Each compound RTP packet except the last one contains a sender report (SR) and a source description (SDES). The last RTCP packet contains an additional BYE packet. Each SR except the last one contains exactly 1 receiver report (RR); the last SR carries no RR.

  The SDES contains CNAME, NAME, and TOOL identifiers.:

  - CNAME is set to *User ID@Proxy*
  - NAME is set to *Display Name* (or *Anonymous* if user blocks caller ID)
  - TOOL is set to the Vendor/Hardware-platform-software-version (such as Cisco/SPA9000-5.2.2(SCb)).
  - The NTP timestamp used in the SR is a snapshot of the Cisco IP phone's local time, not the time reported by an NTP server.
  - If the Cisco IP phone receives a RR from the peer, it tries to compute the round trip delay and show it as the *Call Round Trip Delay* value in the Info section of the web GUI administration page. It can range from 0 to 255 seconds. Defaults to 0 (recommended).
- **No UDP Checksum**—Select yes if you want the Cisco IP phone to calculate the UDP header checksum for SIP messages. Since this involves computation load, you should keep the default value (no) to disable it.

- **Symmetric RTP**—Enable symmetric RTP operation. If enabled, sends RTP packets to the source address and port of the last received valid inbound RTP packet. If disabled (or before the first RTP packet arrives) sends RTP to the destination as indicated in the inbound SDP. Defaults to no.
- **Stats in BYE**—Determines whether the IP phone includes the P-RTP-Stat header or response to a BYE message. The header contains the RTP statistics of the current call. Select yes or no from the drop-down menu. The format of the P-RTP-Stat header is:

  ```
  P-RTP-State: PS=<packets sent>,OS=<octets
  sent>,PR=<packets received>,OR=<octets
  received>,PL=<packets lost>,JI=<jitter in ms>,LA=<delay
  in ms>,DU=<call duration in s>,EN=<encoder>,DE=<decoder>
  ```

  Defaults to no.

STEP 5 Click **Submit All Changes**.

Configuring SDP Payload Types

Configured dynamic payloads are used for outbound calls only when the Cisco IP phone presents an SDP offer. For inbound calls with an SDP offer, the phone follows the caller's assigned dynamic payload type.

Cisco IP phones use the configured codec names in outbound SDP. For incoming SDP with standard payload types of 0-95, the Cisco IP phone ignores the codec names. For dynamic payload types, the Cisco IP phone identifies the codec by the configured codec names (comparison is case-sensitive).

To configure SDP payload types:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **SIP** tab.

STEP 4 Under **SDP Payload Types**, configure the fields shown in the following table and click **Submit All Changes**.

Parameter	Description
AVT Dynamic Payload	AVT dynamic payload type. Ranges from 96-127. Defaults to 101.
INFOREQ Dynamic Payload	This parameter defines the Codec Number used in the SIP messaging for the Dynamic Payload size mechanism. This number should match the number configured in the network/other party to enable the use of Dynamic Payload. The best range is 96-127 for any dynamic payload type. Defaults to blank.
G726r16 Dynamic Payload	G.726-16 dynamic payload type. Ranges from 96-127. Defaults to 98. **NOTE** Not applicable to Cisco SPA 525G.
G726r24 Dynamic Payload	G.726-24 dynamic payload type. Ranges from 96-127. Defaults to 97. **NOTE** Not applicable to Cisco SPA 525G.
G726r32 Dynamic Payload	G726r32 dynamic payload type. The default is 2.
G726r40 Dynamic Payload	G.726-40 dynamic payload type. Ranges from 96-127. Defaults to 96. **NOTE** Not applicable to Cisco SPA 525G.
G729b Dynamic Payload	G729b Dynamic Payload type. Defaults to 99.
EncapRTP Dynamic Payload	EncapRTP Dynamic Payload type. Defaults to 112.
RTP-Start-Loopback Dynamic	RTP-Start-Loopback Dynamic Payload. Defaults to 113.
RTP-Start-Loopback Codec	RTP-Start-Loopback Codec. Select one of following: G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a, or G723. Defaults to G711u.

Parameter	Description
AVT Codec Name	AVT codec name used in SDP. Defaults to telephone-event.
G711u Codec Name	G.711u codec name used in SDP. Defaults to PCMU.
G711a Codec Name	G.711a codec name used in SDP. Defaults to PCMA.
G726r16 Codec Name	G.726-16 codec name used in SDP. Defaults to G726-16. **NOTE** Not applicable to Cisco SPA 525G.
G726r24 Codec Name	G.726-24 codec name used in SDP. Defaults to G726-24. **NOTE** Not applicable to Cisco SPA 525G.
G726r32 Codec Name	G.726-32 codec name used in SDP. Defaults to G726-32.
G726r40 Codec Name	G.726-40 codec name used in SDP. Defaults to G726-40. **NOTE** Not applicable to Cisco SPA 525G.
G729a Codec Name	G.729a codec name used in SDP. Defaults to G729a.
G729b Codec Name	G.729b codec name used in SDP. Defaults to G729ab.
G723 Codec Name	G.723 codec name used in SDP. Defaults to G723. **NOTE** Not applicable to the WIP310 or Cisco SPA 525G.
EncapRTP Codec Name	EncapRTP codec name used in SDP. Defaults to encaprtp.

Configuring SIP Settings for Extensions

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Extension** <number> tab.

STEP 4 Under **Network Settings**, configure the following fields:

Parameter	Description
SIP ToS/DiffServ Value	Time of service (ToS)/differentiated services (DiffServ) field value in UDP IP packets carrying a SIP message. Defaults to 0x68.
SIP CoS Value [0-7]	Class of service (CoS) value for SIP messages. Defaults to 3.
RTP ToS/DiffServ Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. Defaults to 0xb8.
RTP CoS Value [0-7]	CoS value for RTP data. Defaults to 6.
Network Jitter Level	Determines how jitter buffer size is adjusted by the SPA9000. Jitter buffer size is adjusted dynamically. The minimum jitter buffer size is 30 milliseconds or (10 milliseconds + current RTP frame size), whichever is larger, for all jitter level settings. However, the starting jitter buffer size value is larger for higher jitter levels. This setting controls the rate at which the jitter buffer size is adjusted to reach the minimum. Select the appropriate setting: low, medium, high, very high, or extremely high. Defaults to high.
Jitter Buffer Adjustment	Controls how the jitter buffer should be adjusted. Select the appropriate setting: up and down, up only, down only, or disable. Defaults to up and down.

STEP 5 Under **SIP Settings**, configure the following fields:

Parameter	Description
SIP Transport	Select from UDP, TCP, or TLS. Defaults to UDP.
SIP Port	Port number of the SIP message listening and transmission port. Defaults to 5060.
SIP 100REL Enable	To enable the support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests, select yes. Otherwise, select no. Defaults to no.
EXT SIP Port	The external SIP port number.
Auth Resync-Reboot	If this feature is enabled, the Cisco IP phone authenticates the sender when it receives a NOTIFY message with the following requests: ▪ resync ▪ reboot ▪ report ▪ restart ▪ XML-service To use this feature, select **yes**. Otherwise, select **no**. Defaults to yes.
SIP Proxy-Require	The SIP proxy can support a specific extension or behavior when it sees this header from the user agent. If this field is configured and the proxy does not support it, it responds with the message, unsupported. Enter the appropriate header in the field provided.
SIP Remote-Party-ID	To use the Remote-Party-ID header instead of the From header, select yes. Otherwise, select no. Defaults to yes.

Parameter	Description
Referror Bye Delay	Controls when the Cisco IP phone sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referror, Refer Target, Referee, and Refer-To Target) are configured on this screen. For the Referror Bye Delay, enter the appropriate period of time in seconds. Defaults to 4.
Refer-To Target Contact	To contact the refer-to target, select yes. Otherwise, select no. Default: no.
Referee Bye Delay	For the Referee Bye Delay, enter the appropriate period of time in seconds. Defaults to 0.

Parameter	Description
SIP Debug Option	SIP messages are received at or sent from the proxy listen port. This feature controls which SIP messages to log. Choices are as follows: ▪ none—No logging. ▪ 1-line—Logs the start-line only for all messages. ▪ 1-line excl. OPT—Logs the start-line only for all messages except OPTIONS requests/responses. ▪ 1-line excl. NTFY—Logs the start-line only for all messages except NOTIFY requests/responses. ▪ 1-line excl. REG—Logs the start-line only for all messages except REGISTER requests/responses. ▪ 1-line excl. OPT|NTFY|REG—Logs the start-line only for all messages except OPTIONS, NOTIFY, and REGISTER requests/responses. ▪ full—Logs all SIP messages in full text. ▪ full excl. OPT—Logs all SIP messages in full text except OPTIONS requests/responses. ▪ full excl. NTFY—Logs all SIP messages in full text except NOTIFY requests/responses. ▪ full excl. REG—Logs all SIP messages in full text except REGISTER requests/responses. ▪ full excl. OPT|NTFY|REG—Logs all SIP messages in full text except for OPTIONS, NOTIFY, and REGISTER requests/responses. Defaults to none.
Refer Target Bye Delay	For the Refer Target Bye Delay, enter the appropriate period of time in seconds. Defaults to 0.
Sticky 183	If this feature is enabled, the IP telephony ignores further 180 SIP responses after receiving the first 183 SIP response for an outbound INVITE. To enable this feature, select yes. Otherwise, select no. Defaults to no.

Parameter	Description
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy. **NOTE** Not applicable to the WIP310.
Ntfy Refer On 1xx-To-Inv	If set to **yes**, as a transferee, the phone will send a NOTIFY with Event:Refer to the transferor for any 1xx response returned by the transfer target, on the transfer call leg. If set to **no**, the phone will only send a NOTIFY for final responses (200 and higher). **NOTE** Not applicable to the WIP310.
Use Anonymous with RPID	This parameter applies only if <SIP Remote-Party-ID> is set to **yes**; otherwise, it is ignored. If the parameter is set to **yes**, the FROM header's display-name and user-id fields are set to anonymous when the caller blocks his caller-id. If the parameter is set to **no**, the FROM header's display-name and user-id are not masked. The Remote-Party-ID header indicates privacy=full when the caller wishes to block his caller-id. Default: yes. **NOTE** Not applicable to the WIP310.
Set G729 annexb	Configure G.729 Annex B settings. **NOTE** Not applicable to the Cisco SPA 525G.

STEP 6 Click **Submit All Changes**.

Configuring a SIP Proxy Server

To configure SIP proxy and registration parameters:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Extension** <number> tab.

STEP 4 Configure the proxy and registration parameters for each extension.

Parameter	Description
Proxy	SIP proxy server and port number set by the service provider for all outbound requests. For example: 192.168.2.100:6060. **NOTE** Port number is optional. The default is port 5060.
Use Outbound Proxy	Enables an outbound proxy (for example, 172.20.2.1:5060—port is optional) or a domain name such as sip.server.com as long as this name is a fully-qualified domain name. If set to no, the Outbound Proxy and Use OB Proxy in Dialog fields are ignored. Defaults to no. Optionally, the proxy can be configured (Cisco SPA 500 series only) for Survivable Remote Site Telephony (SRST) support. The proxy is configured with an extension that includes a statically-configured DNS SRV record or DNS A record. Configuring the proxy allows for failover and fallback functionality with a secondary proxy server. For example: **For SRV Record:** sip.server.com:SRV=node1.sip.server.com:5060:p=1:w=50|node2.sip.server.com:5060:p=2:w=50 **NOTE** Set "Use DNS SRV" to **no** and "DNS SRV Auto Prefix" to **no**. **For A Record:** sip.server.com:A=172.20.2.1,172.20.2.2 **NOTE** Set "Use DNS SRV" to **no** and "DNS SRV Auto Prefix" to **no**.
Outbound Proxy	SIP outbound proxy server where all outbound requests are sent as the first hop.
Use OB Proxy In Dialog	Select yes for SIP requests to be sent to the outbound proxy within a dialog. This field is ignored if: ▪ Use Outbound Proxy is set to no or ▪ Outbound Proxy is blank Defaults to yes.

Parameter	Description
Register	Enables periodic registration with the proxy. This parameter is ignored if a proxy is not specified. Defaults to yes.
Make Call Without Reg	Enables making outbound calls without successful (dynamic) registration by the phone. If set to no, the dial tone plays only when registration is successful. Defaults to no.
Register Expires	Defines how often the phone renews registration with the proxy. If the proxy responds to a REGISTER with a lower expires value, the phone renews registration based on that lower value instead of the configured value. If registration fails with an “Expires too brief” error response, the phone retries with the value specified in the Min-Expires header of the error. Defaults to 60 seconds.
Ans Call Without Reg	If enabled, the user does not have to be registered with the proxy to answer calls. Defaults to no.
Use DNS SRV	Enables DNS SRV lookup for the proxy and outbound proxy. Defaults to no.
DNS SRV Auto Prefix	Enables the phone to automatically prepend the proxy or outbound proxy name with _sip._udp when performing a DNS SRV lookup on that name. Defaults to no.
Proxy Fallback Intvl	Sets the delay after which the phone retries from the highest priority proxy (or outbound proxy) after it has failed over to a lower priority server. The phone should have the primary and backup proxy server list via DNS SRV record lookup on the server name. It needs to know proxy priority; otherwise, it does not retry. Defaults to 3600 seconds.

Parameter	Description
Proxy Redundancy Method	Select Normal or Based on SRV port. The phone creates an internal list of proxies returned in the DNS SRV records. If you select Normal, the list contains proxies ranked by weight and priority. If you select Based on SRV, the phone uses normal, then inspects the port number based on the first-listed proxy port. Defaults to Normal.

STEP 5 Click **Submit All Changes**.

Configuring Subscriber Information Parameters

To configure subscriber information parameters for each extension:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Ext** <number> tab.

STEP 4 Enter the subscriber information:

Parameter	Description
Display Name	Display name for caller ID.
User ID	Extension number for this line.
Password	Password for this line. Defaults to blank.
Use Auth ID	To use the authentication ID and password for SIP authentication, select yes. Otherwise, select no to use the user ID and password. Defaults to no.

Parameter	Description
Auth ID	Authentication ID for SIP authentication. Defaults to blank.
Mini Certificate	Base64 encoded of Mini-Certificate concatenated with the 1024-bit public key of the CA signing the MC of all subscribers in the group. Defaults to blank.
SRTP Private Key	Base64 encoded of the 512-bit private key per subscriber for establishment of a secure call. Defaults to blank.

STEP 5 Click **Submit All Changes**.

Configuring SPCP on the Cisco SPA 525G

The Cisco SPA 525G can be used as part of a Cisco Unified Communications System. This system uses SPCP (also called SCCP) for call control features.

To configure SPCP on the Cisco SPA 525G:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Under **System Configuration**, in the **SPA525-protocol field**, choose **SCCP**.

STEP 5 (Optional) To configure the phone to automatically detect the protocol being used on the network to which it is connected, in the **SPA525-auto-detect-sccp** field, choose **yes**.

STEP 6 Click **Submit All Changes**.

Configuring SPCP on the Cisco SPA 50XG

The Cisco SPA 50XG can be used as part of a Cisco Unified Communications System. This system uses SPCP (also called SCCP) for call control features.

To configure SPCP on the Cisco SPA 50XG:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Under **System Configuration**, in the **Signaling Protocol** field, choose **SCCP**.

STEP 5 (Optional) To configure the phone to automatically detect the protocol being used on the network to which it is connected, in the **SPCP Auto-detect** field, choose **yes**.

STEP 6 Click **Submit All Changes**.

NOTE For the Cisco SPA501G, can be configured using the IVR. See the **"Using IVR on the Cisco SPA 501G IP Phone" section on page 17**.

Network Address Translation (NAT) and Cisco IP Phones

NAT is a function that allows multiple devices to share the same public, routable, IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP addresses. To enable VoIP to co-exist with NAT, some form of NAT traversal is required.

Some ITSPs provide NAT traversal, but some do not. If your ITSP does not provide NAT traversal, you have several options.

NAT Mapping with Session Border Controller

It is strongly recommended that you choose an ITSP that supports NAT mapping through a Session Border Controller. With NAT mapping provided by the ITSP, you have more choices in selecting a router.

NAT Mapping with SIP-ALG Router

If the ITSP network does not provide a Session Border Controller functionality, you can achieve NAT mapping by using a router that has a SIP ALG (Application Layer Gateway). By using a SIP-ALG router, you have more choices in selecting an ITSP.

Configuring NAT Mapping with a Static IP Address

If the ITSP network does not provide a Session Border Controller functionality, and if other requirements are met, you can configure NAT mapping to ensure interoperability with the ITSP.

Requirements

- You must have an external (public) IP address that is static.
- The NAT mechanism used in the router must be symmetric. See **"Determining Whether the Router Uses Symmetric or Asymmetric NAT," on page 108**.

NOTE Use NAT mapping only if the ITSP network does not provide a Session Border Controller functionality.

STEP 1 Click **Admin Login** and **advanced**.

STEP 2 Click the **SIP** tab.

STEP 3 Under **NAT Support Parameters**, configure the following:

- **Handle VIA received, Insert VIA received, Substitute VIA Addr:** yes
- **Handle VIA rport, Insert VIA rport, Send Resp To Src Port:** yes
- **EXT IP:** Enter the public IP address for your router.

STEP 4 Click the **Ext** <number> tab. Configure the following:

- **NAT Mapping Enable:** Choose **yes**.
- **NAT Keep Alive Enable:** Choose **yes** (optional).

STEP 5 Click **Submit All Changes**.

NOTE You also need to configure the firewall settings on your router to allow SIP traffic. See **"Configuring SIP," on page 83**.

Configuring NAT Mapping with STUN

If the ITSP network does not provide a Session Border Controller functionality, and if other requirements are met, it is possible to use STUN as a mechanism to discover the NAT mapping. This option is considered a practice of last resort and should be used only if the other methods are unavailable.

Requirements

- STUN is a viable option only if your router uses asymmetric NAT. See **"Determining Whether the Router Uses Symmetric or Asymmetric NAT," on page 108**.
- You must have a computer running STUN server software. You can use a public STUN server or set up your own STUN server.

NOTE Use NAT mapping only if the ITSP network does not provide a Session Border Controller functionality.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **SIP** tab.

STEP 4 Under **NAT Support Parameters**, configure the following:

- **Handle VIA received:** yes
- **Handle VIA rport:** yes
- **Insert VIA received:** yes
- **Insert VIA rport:** yes
- **Substitute VIA Addr:** yes
- **Send Resp To Src Port:** yes
- **STUN Enable**: Choose **yes**.
- **STUN Server:** Enter the IP address for your STUN server.

STEP 5 Click the **Ext** <number> tab. Configure the following:

- **NAT Mapping Enable:** Choose **yes**.
- **NAT Keep Alive Enable:** Choose **yes** (optional).

NOTE Your ITSP may require the phone to send NAT keep alive messages to keep the NAT ports open permanently. Check with your ITSP to determine the requirements.

STEP 6 Click **Submit All Changes**.

NOTE You also need to configure the firewall settings on your router to allow SIP traffic. See **"Configuring SIP," on page 83**.

Determining Whether the Router Uses Symmetric or Asymmetric NAT

STUN does not work on routers with symmetric NAT. With symmetric NAT, IP addresses are mapped from one internal IP address and port to one external, routable destination IP address and port. If another packet is sent from the same source IP address and port to a different destination, then a different IP address and port number combination is used. This method is restrictive because an external host can send a packet to a particular port on the internal host *only if* the internal host first sent a packet from that port to the external host.

NOTE This procedure assumes that a syslog server is configured and is ready to receive syslog messages.

STEP 1 Make sure you do not have firewall running on your PC that could block the syslog port (by default this is 514).

STEP 2 Log on to the phone's web UI. For information about this, see the **"Using the Web Administration User Interface" section on page 11**.

STEP 3 Click **Admin Login > Advanced**. (For WIP310, click **Admin Login**.)

STEP 4 Click the **System** tab, then set *Debug Server* to the IP address and port number of your syslog server. Note that this address and port number has to be reachable from the Cisco IP phone. This port number appears on the output file name. The default port number is 514. The default output is named syslog.514.log (if port number was not specified).

STEP 5 Set *Debug Level* to **3.** Do not change the value of the *Syslog Server* parameter.

STEP 6 To capture SIP signaling messages, click the **Ext** tab.

STEP 7 Set *SIP Debug Option* to **Full**.

STEP 8 To collect information about what type of NAT your router uses click the **SIP** tab and scroll to NAT Support Parameters.

STEP 9 Back in the *SIP* tab, select **yes** in the *STUN Test Enable* drop-down box.

View the debug messages to determine if your network uses symmetric NAT. Look for the Warning header in REGISTER messages, for example, Warning: 399 Spa "Full Cone NAT detected."

STEP 10 Click **Submit All Changes**.

5

Configuring Security, Quality, and Network Features

This chapter describes how to configure security, quality, and network features for the phone. It contains the following sections:

Setting Security Features

The following features help ensure that calls are secure and authenticated.

SIP Initial INVITE and MWI Challenge

SIP INVITE (initial) and MWI message in a session can be challenged by the endpoint. The purpose of this challenge is to restrict the SIP servers that are permitted to interact with the devices on the service provider network, which significantly increases the security of the VoIP network by preventing malicious attacks against the device.

To configure SIP INVITE challenge:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click **Ext** <number>, then scroll to the *SIP Settings* section.

STEP 4 In the Auth INVITE field, choose **yes**.

STEP 5 Click **Submit All Changes**.

SIP Over TLS

Transport layer security (TLS) is a standard protocol for securing and authenticating communications over the Internet.

SIP Over TLS eliminates the possibility of malicious activity by encrypting the SIP messages by the SIP proxy of the service provider and the end user. SIP Over TLS relies on the widely-deployed and standardized Transport Layer Security (TLS) protocol. Note that SIP Over TLS encrypts only the signaling messages and not the media. A separate secure protocol such as Secure Real-Time Transport Protocol (SRTP) (see below) can be used to encrypt voice packets.

The TLS protocol has two layers:

- TLS Record Protocol -- layered on top of a reliable transport protocol, such as SIP or TCH, it ensures that the connection is private by using symmetric data encryption and it ensures that the connection is reliable.
- TLS Handshake Protocol -- allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

TLS is application protocol-independent. Higher-level protocols such as SIP can layer on top of the TLS protocol transparently.

The IP phones use UDP as a standard for SIP transport, but they also support SIP over TLS for added security.

To enable TLS for the phone:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click **Ext** <number>, then scroll to the *SIP Settings* section.

STEP 4 Select **TLS** from the *SIP Transport* drop-down box.

STEP 5 Click **Submit All Changes**.

SRTP and Securing Calls

Secure Real-Time Transport Protocol (SRTP) is a secure protocol for transporting real-time data over networks. Cisco SPA 500 Series and Wireless IP Phones use SRTP to securely send and receive real-time voice traffic from other phones and gateways. Security Description (RFC 4568) is supported.

SRTP provides media encryption to ensure that media streams between devices are secure and that only the intended devices receive and read the data.

When a call is secure, the voice conversation is encrypted so that others cannot eavesdrop on the conversation. To enable this feature the IP phone must have a mini-certificate installed.

The supplementary service Secure All Calls (*16)—Defaults to prefer to use encrypted media (voice codecs). Audio packets in both directions of outbound calls are encrypted using SRTP.

To use Secure Call on an extension, you must configure *Mini Certificate* and *SRTP Private Key* for that extension. These parameters appear on the *Ext* tabs.

Secure Call Service activates secure encryption of RTP streams between the two endpoints. You can disable this if the other endpoint (or gateway) does not support this proprietary method.

To enable the secure call service:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Phone** tab.

STEP 4 In the **Supplementary Services** section, under **Secure Call Serv,** choose **yes**.

STEP 5 Click **Submit All Changes**.

NOTE This feature can also be configured from the **User** tab, under **Supplementary Services**.

Users can enter *18 to Secure Next Call—Uses encrypted media for the next outbound call (on this call appearance only). This star code is redundant if all outbound calls are secure by default.

The phone can be configured for secure provisioning using the factory-installed security certificate. To determine if the **Client Certificate** is installed on the phone:

- SPA 50XG: Press the **Setup** button and select **Product Info**. Scroll to **Client Cert**.
- SPA 525G: Press the **Setup** button and select **Status**. Select **Product Information**. Scroll to **Certificate**.
- WIP310: Log in to the web administration interface. In the **Info** tab, under **Product Information**, certificate information is listed in the **Client Certificate** field.

Secure Call Indication Tone

This tone is played when a call has been successfully switched to secure mode. It should be played only for a short while (less than 30 seconds) and at a reduced level (less than -19 dBm), so it does not interfere with the conversation. You can configure it on the *Regional* web page under *Call Progress Tones*.

Defaults to 397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2)

Ensuring Voice Quality

Voice quality perceived by the subscribers of the IP Telephony service should be indistinguishable from that of the PSTN. Cisco IP phones support several codecs. See:

- **"Supported Codecs" section on page 114**
- **"Bandwidth Requirements" section on page 115**
- **"Factors Affecting Voice Quality" section on page 116**

Supported Codecs

Negotiation of the optimal voice codec sometimes depends on the ability of the Cisco IP Phone to "match" a codec name with the far-end device/gateway codec name. Cisco IP phones allow the network administrator to individually name the various codecs that are supported such that the correct codec successfully negotiates with the far-end equipment.

Note that Cisco IP phones support voice codec priority. You can select up to three preferred codecs.

The administrator can select the low-bit-rate codec used for each line. G.711a and G.711u are always enabled. The following table shows the codecs supported by Cisco IP phones. The third column shows the voice quality Mean Opinion Score (MOS), with a scale of 1–5, in which higher is better.

Codec (Voice Compression Algorithm)	Complexity and Description	MOS Score
G.711 (A-law and u-law)	Very low complexity. Supports uncompressed 64 kbps digitized voice transmission at one through ten 5 ms voice frames per packet. This codec provides the highest voice quality and uses the most bandwidth of any of the available codecs.	4.5 Highest voice quality

Codec (Voice Compression Algorithm)	Complexity and Description	MOS Score
G.726	Low complexity. Supports compressed 16, 24, 32, and 40 kbps digitized voice transmission at one through ten 10 ms voice frames per packet. When no static payload value is assigned per RFC 1890, Cisco IP phones can support dynamic payloads for G.726. **NOTE** G.726 is supported only for 32kbps on the SPA 525G.	4.1 (32 kbps)
G.729 and G.729A	G.729A low-medium complexity. G.729 medium complexity. G.729A requires about half the processing power of G.729. The G.729 and G.729A bit streams are compatible and interoperable, but not identical.	4
G.723.1	High complexity. Cisco IP phones support the use of ITU G.723.1 audio codec at 6.4 kbps. Up to two channels of G.723.1 can be used simultaneously. For example, Line 1 and Line 2 can be using G.723.1 simultaneously, or Line 1 or Line 2 can initiate a three-way conference with both call legs using G.723.1. **NOTE** G.723.1 is not supported on the 525G or WIP310.	3.8
G.722	Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio. **NOTE** Not supported on the WIP310.	4.3 (approx)

Bandwidth Requirements

Depending on how you have your IP phones configured, each call requires 55 to 110 kbps in each direction. Therefore, using G.729 as the voice codec setting, and with an average business-grade broadband Internet connection supporting 1.5 Mbps downstream and 384 kbps upstream, a total of seven (7) simultaneous conversations can be reliably supported with adequate bandwidth available for file downloads.

Cisco recommends using the Cisco IP phones with QoS-capable networking equipment that can prioritize the VoIP application traffic. QoS features are available on many data networking switches and routers. A QoS-enabled router prioritizes the packets going upstream to the ISP.

The following table approximates the bandwidth budget for each side of the conversation (in each direction) using different codecs and number of calls. This table is based on the following assumptions:

- Bandwidth calculated with no silence suppression
- 20 millisecond of payload per RTP packet

Codec	Est. Bandwidth Budget	2 Calls	4 Calls	6 Calls	8 Calls
G.711	110 kbps	220 kbps	440 kbps	660 kbps	880 kbps
G.722	110 kbps	220 kbps	440 kbps	660 kbps	880 kbps
G.726-40	87 kbps	174 kbps	348 kbps	522 kbps	696 kbps
G.726-32	79 kbps	158 kbps	316 kbps	474 kbps	632 kbps
G.726-24	71 kbps	142 kbps	284 kbps	426 kbps	568 kbps
G.726-16	63 kbps	126 kbps	252 kbps	378 kbps	504 kbps
G.729	55 kbps	110 kbps	220 kbps	330 kbps	440 kbps

NOTE The use of silence suppression can reduce the average bandwidth budget by 30% or more.

For more information about bandwidth calculation, refer to the following websites:

http://www.erlang.com/calculator/lipb/

http://www.packetizer.com/voip/diagnostics/bandcalc.html

Factors Affecting Voice Quality

The following factors contribute to voice quality:

- Audio compression algorithm—Speech signals are sampled, quantized, and compressed before they are packetized and transmitted to the other end. For IP Telephony, speech signals are usually sampled at 8000 samples per second with 12–16 bits per sample. The compression algorithm plays a large role in determining the voice quality of the reconstructed speech

signal at the other end. Cisco IP phones support the most popular audio compression algorithms for IP Telephony: G.711 a-law and u-law, G.726, G.729a, G.722 (not supported on WIP310) and G.723.1. (not supported on the SPA 525G or WIP310.)

- The encoder and decoder pair in a compression algorithm is known as a codec. The compression ratio of a codec is expressed in terms of the bit rate of the compressed speech. The lower the bit rate, the smaller the bandwidth required to transmit the audio packets. Although voice quality is usually lower with a lower bit rate, it is usually higher as the complexity of the codec gets higher at the same bit rate.
- Silence suppression—Cisco IP phones apply silence suppression so that silence packets are not sent to the other end to conserve more transmission bandwidth. IP bandwidth is used only when someone is speaking. Voice activity detection (VAD) with silence suppression is a means of increasing the number of calls supported by the network by reducing the required bidirectional bandwidth for a single call. A noise level measurement is sent periodically during silence suppressed intervals so that the other end can generate artificial comfort noise (comfort noise generator, or CNG).
- Packet loss—Audio packets are transported by UDP, which does not guarantee the delivery of the packets. Packets may be lost or contain errors that can lead to audio sample drop-outs and distortions and lower the perceived voice quality. The Cisco SPA 500 Series and Wireless IP Phones apply an error concealment algorithm to alleviate the effect of packet loss.
- Network jitter—The IP network can induce varying delay of received packets. The RTP receiver in Cisco IP phones keeps a reserve of samples to absorb the network jitter, instead of playing out all the samples as soon

as they arrive. This reserve is known as a jitter buffer. The bigger the jitter buffer, the more jitter it can absorb, but this also introduces bigger delay.

Jitter buffer size should be kept to a relatively small size whenever possible. If jitter buffer size is too small, many late packets may be considered as lost and thus lowers the voice quality. Cisco IP phones dynamically adjust the size of the jitter buffer according to the network conditions that exist during a call.

The minimum jitter buffer size is 30 milliseconds or (10 milliseconds + current RTP frame size), whichever is larger, for all jitter level settings. However, the starting jitter buffer size value is larger for higher jitter levels. This setting controls the rate at which the jitter buffer size is adjusted to reach the minimum. Select the appropriate setting: low, medium, high, very high, or extremely high. Defaults to high.

Jitter Buffer Adjustment—Controls how the jitter buffer should be adjusted. Select the appropriate setting: up and down, up only, down only, or disable. Defaults to up and down.

- Echo—Impedance mismatch between the telephone and the IP Telephony gateway phone port can lead to near-end echo. Cisco IP phones have a near-end echo canceller with at least 8 ms tail length to compensate for impedance match. Cisco IP phones implement an echo suppressor with comfort noise generator (CNG) so that any residual echo is not noticeable.
- Hardware noise—Certain levels of noise can be coupled into the conversational audio signals because of the hardware design. The source can be ambient noise or 60 Hz noise from the power adaptor. The Cisco hardware design minimizes noise coupling.
- End-to-end delay—End-to-end delay does not affect voice quality directly but is an important factor in determining whether IP phone subscribers can interact normally in a conversation. A reasonable delay should be about 50–100 ms. End-to-end delay larger than 300 ms is unacceptable to most callers. Cisco IP phones support end-to-end delays well within acceptable thresholds.
- Adjustable Audio Frames Per Packet—Allows you to set the number of audio frames contained in one RTP packet. Packets can be adjusted to contain from 1–10 audio frames. Increasing the number of frames decreases the bandwidth utilized, but it also increases delay and can affect voice quality.

Configuring Voice Codecs

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. If the G.729a codec is enabled and included in the codec list, that resource is tied up until the end of the call whether or not the call actually uses G.729a. If the G729a resource is already allocated (and since only one G.729a resource is allowed per IP phone), no other low-bit-rate codec can be allocated for subsequent calls. The only choices are G711a and G711u.

Since two G.723.1/G.726 resources are available per IP phone, you should disable the use of G.729a to guarantee support for two simultaneous G.723/G.726 codecs.

To configure the voice codecs on each extension:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Ext** <number> tab for the extension you want to configure.

STEP 4 Under **Audio Configuration**, configure the following parameters:

Parameter	Description
Preferred Codec	Preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following: ▪ G711u (all models) ▪ G711a (all models) ▪ G726-16 (not supported on WIP310, SPA 525G) ▪ G726-24 (not supported on WIP310, SPA 525G) ▪ G726-32 ▪ G726-40 (not supported on WIP310, SPA 525G) ▪ G729a ▪ G723 (not supported on WIP310, SPA 525G) ▪ G722 (not supported on WIP310) See **"Supported Codecs" section on page 114**. Defaults to G711u.
Use Pref Codec Only	To use only the preferred codecs for all calls, select yes. (The call fails if the far end does not support these codecs.) Otherwise, select no. Defaults to no.
Second Preferred Codec	If the first codec fails, this codec is tried. Defaults to unspecified. **NOTE** Not applicable to the WIP310.
Third Preferred Codec	If the second codec fails, this codec is tried. Defaults to unspecified. **NOTE** Not applicable to the WIP310.
G729a Enable	To enable the use of the G.729a codec at 8 kbps, select yes. Otherwise, select no. Defaults to yes.
G722 Enable	Enables use of the G.722 codec. Defaults to yes. **NOTE** Not applicable to the WIP310.

Parameter	Description
G723 Enable	To enable the use of the G.723a codec at 6.3 kbps, select yes. Otherwise, select no. Defaults to yes. **NOTE** Not applicable to the WIP310 or SPA 525G.
G726-16 Enable	To enable the use of the G.726 codec at 16 kbps, select yes. Otherwise, select no. Defaults to yes. **NOTE** Not applicable to the WIP310 or SPA 525G.
G726-24 Enable	To enable the use of the G.726 codec at 24 kbps, select yes. Otherwise, select no. Defaults to yes. **NOTE** Not applicable to the WIP310 or SPA 525G.
G726-32 Enable	To enable the use of the G.726 codec at 32 kbps, select yes. Otherwise, select no. Defaults to yes.
G726-40 Enable	To enable the use of the G.726 codec at 40 kbps, select yes. Otherwise, select no. Defaults to yes. **NOTE** Not applicable to the WIP310 or SPA 525G.
Release Unused Codec	Allows the release of codecs not used after codec negotiation on the first call so that other codecs can be used for the second line. To use this feature, select yes. Defaults to yes.
DTMF Process AVT	Select yes to process RTP DTMF events. Otherwise, select no. If this parameter is set to no, the AVT payload type is not included in outbound SDP. Defaults to yes.
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select yes. Otherwise, select no. See **"Ensuring Voice Quality" section on page 114**. Defaults to no.

Parameter	Description
DTMF Tx Method	Select the method to transmit DTMF signals to the far end: InBand, audio video transport (AVT), INFO, Auto, InBand+INFO, or AVT+INFO. InBand sends DTMF using the audio path. AVT sends DTMF as AVT events. INFO uses the SIP INFO method. Auto uses InBand or AVT based on the outcome of codec negotiation. Defaults to Auto.
DTMF Tx Volume for AVT Packet	Allows you to manually configure the AVT Tx volume. The value of this parameter is inserted into the volume field of the payload in the AVT packet. Values are based on the AVT specification as described in RFC 2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*. According to RFC 2833, the volume field is represented by 6 bits, and describes the power level of the tone, expressed in dBm0 after dropping the sign. Valid range for this parameter is 0 to 63. If the provisioned value is negative, it will be negated first. Thereafter, if the value is beyond the high limit of 63, it will be clipped to 63. The default value is 0, and is the recommended setting. However, some gateways do not accept this volume setting. If the gateway does not accept the value of 0, the DTMF tone is not relayed to the remote end. As a workaround for the phone to interoperate with those gateways, you can change the value to a value greater than 0.

STEP 5 Click **Submit All Changes**.

Configuring Domain and Internet Settings

Configuring Restricted Access Domains

You can configure restricted access domains. If you enter domains, the Cisco IP phones respond to SIP messages only from the entered servers.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Enter fully-qualified domain names (FQDNs) for each SIP server you want the phone to respond to. Separate with semicolons.

STEP 5 Click **Submit All Changes**.

Configuring DHCP, Static IP, and PPPoE Information

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Configure the Internet Connection Type. Choose one of the following:

- Dynamic Host Configuration Protocol (DHCP): Configure the phone to receive an IP address from the network DHCP. Cisco IP phones typically operate in a network where a DHCP server assigns the device its IP address. Because IP addresses are a limited resource, the DHCP server periodically renews the device lease on the IP address. If a phone loses its IP address for any reason, or if some other device on the network is assigned its IP address, the communication between the SIP proxy and the phone is either severed or degraded. Whenever an expected SIP response is not received within a programmable amount of time after the corresponding SIP command is sent, the *DHCP Timeout on Renewal* feature causes the device to request a renewal of its IP address. If the DHCP server returns the IP address that it originally assigned to the phone, the DHCP assignment is presumed to be operating correctly. Otherwise, the phone resets to try to fix the issue.
- Static IP—Configure a static IP address for the phone.
- PPPoE—Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device, or cable modem. All users on an Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.

NOTE PPPoE is not applicable to WIP310.

STEP 5 Click **Submit All Changes**.

NOTE For the SPA501G, can be configured using the IVR. See the **"Using IVR on the Cisco SPA 501G IP Phone" section on page 17**.

Setting a Static IP Address

If you configured Static IP as the internet connection type:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Configure the following fields:

- Static IP Address—Enter the static IP address of the phone.
- Netmask—Enter the subnet mask of the phone.
- Gateway—Enter the IP address of the gateway.

For the SPA 525G, you also have the following fields available:

- LAN MTU—LAN Maximum Transmission Unit size. Default value: 1500.
- Duplex Mode—Choose one of the following to configure the speed/duplex for the phone's Ethernet ports:
  - Auto
  - 10MBps/Duplex
  - 10MBps/Half
  - 100Mbps/Duplex
  - 100MBps/Half

STEP 5 Click **Submit All Changes**.

NOTE For the SPA501G, can be configured using the IVR. See the **"Using IVR on the Cisco SPA 501G IP Phone" section on page 17**.

Configuring PPPoE Settings

If you configured PPPoE as the internet connection type:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Configure the following fields:

Parameter	Description
PPPoE Login Name	Specifies the account name assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.
PPPoE Login Password	Specifies the password assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.
PPPoE Service Name	Specifies the service name assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.

STEP 5 Click **Submit All Changes**.

Setting Optional Network Parameters

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Configure the following fields:

Parameter	Description
Host Name	The host name of the phone.
Domain	The network domain of the phone. However, if using LDAP, see **Configuring Lightweight Directory Access Protocol (LDAP) for the Cisco SPA 500 Series, page 67**.
Primary DNS	DNS server used by the phone in addition to DHCP supplied DNS servers if DHCP is enabled; when DHCP is disabled, this is the primary DNS server. Defaults to 0.0.0.0. However, if using LDAP, see **Configuring Lightweight Directory Access Protocol (LDAP) for the Cisco SPA 500 Series, page 67**.
Secondary DNS	DNS server used by the phone in addition to DHCP supplied DNS servers if DHCP is enabled; when DHCP is disabled, this is the secondary DNS server. Defaults to 0.0.0.0.
DNS Server Order	Specifies the method for selecting the DNS server. The options are Manual, Manual/DHCP, and DHCP/Manual.
DNS Query Mode	Do parallel or sequential DNS Query. With parallel DNS query mode, the phone sends the same request to all the DNS servers at the same time when doing a DNS lookup, the first incoming reply is accepted by the phone. Defaults to parallel. Not available on WIP310.

Parameter	Description
Syslog Server	Specify the syslog server name and port. This feature specifies the server for logging system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.
Debug Server	The debug server name and port. This feature specifies the server for logging debug information. The level of detailed output depends on the debug level parameter setting.
Debug Level	The debug level from 0-3. The higher the level, the more debug information is generated. Zero (0) means no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Defaults to 0.
NTP Enable	Enables Network Time Protocol (NTP). Applies to the SPA 525G only.
Primary NTP Server	IP address or name of primary NTP server. The phones use these servers to synchronize its time. Defaults to blank.
Secondary NTP Server	IP address or name of secondary NTP server. The phones use these servers to synchronize its time. Defaults to blank.

STEP 5 Click **Submit All Changes.**

Configuring VLAN Settings

Using the IP Phones in a VLAN

If you use a VLAN your IP phone voice packets are tagged with the VLAN ID. (This section is not applicable to the WIP310.)

If you are using a Cisco switch, Cisco discovery protocol (CDP) is enabled (this is the default). CDP is negotiation-based and determines which VLAN the IP phone resides in. CDP:

- Obtains the protocol addresses of neighboring devices and also discovers the platform of those devices.
- Shows information about the interfaces your router uses.
- Is media and protocol-independent.

If you are using a VLAN without CDP, you must enter a VLAN ID for the IP phone.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **System** tab.

STEP 4 Enter the following parameters:

Parameter	Description
Enable VLAN	Choose **Yes** to enable VLAN. Choose **no** to disable.
Enable CDP	*Enable CDP* only if you are using a switch that has Cisco Discovery Protocol. CDP is negotiation based and determines which VLAN the IP phone resides in.
VLAN ID	If you use a VLAN without CDP (VLAN enabled and CDP disabled), enter a *VLAN ID* for the IP phone. Note that only voice packets are tagged with the VLAN ID.
Enable PC Port VLAN Tagging	Enables VLAN and priority tagging on the phone data port (802.1p/q). This feature facilities tagging of the VLAN ID (802.1Q) and priority bits (802.1p) of the traffic coming from the PC port of the IP phone. Defaults to No. Choose **Yes** to enable the tagging algorithm.
PC Port VLAN Highest Priority	Choose **No Limit**, or 0-7 (default 0). The highest priority is 7. The priority applied to all frames, tagged and untagged. The phone modifies the frame priority only if the incoming frame priority is higher than this value.

Parameter	Description
PC Port VLAN ID	0-4095 (default 0). Value of the VLAN ID. The phone tags all the untagged frames coming from the PC (it will not tag frames with an existing tag).

STEP 5 Click **Submit All Changes**.

Configuring SSL VPN on the Cisco SPA 525G

The Cisco SPA 525G can be used in a virtual private network (VPN) to allow users secure access to the office phone network from remote locations. Users can connect their Cisco SPA 525G phones to the Internet and then use the VPN feature to securely access the company phone network. This feature works on the Cisco SPA 525G IP Phone using both SIP and SPCP.

The Cisco SPA 525G works with the Cisco AnyConnect VPN client and the following VPN devices:

- Cisco 500 Series Secure Router
- Cisco 5500 Series Adaptive Security Appliance
- Cisco Unified Communications 520 Series

You must configure the SSL VPN device to ensure proper routing of voice data with desired VLAN and QoS at the end of the SSL VPN server. The following restrictions apply:

- HTTP proxy is not supported.
- SSL client certificate verification is not supported.
- CDP and VLAN tagging and QoS for the voice and PC port are not supported on the SSL VPN tunnel.

Because using the VPN requires internal phone resources, performance can suffer if using memory-intensive applications or configurations on the phone when the phone is connected using the VPN. The following restrictions apply:

- Only the G.711 Audio Codec is supported.
- SRTP for secured audio is not supported.

- Video monitoring is not supported.

To configure and use the Cisco SPA 525G on a VPN, you must do the following:

1. Configure the VPN on the VPN server using Cisco AnyConnect VPN client software.
2. Configure the VPN administrative settings on the Cisco SPA 500 Series IP phone using the administration web user interface.
3. Configure the VPN user settings on the administration web user interface or on the IP phone using the phone menu.

Configuring the VPN on the Security Appliance

NOTE Specific configuration instructions are not presented in this document. For detailed instructions for your particular device, see the application notes in the Cisco Small Business Support Community.

STEP 1 Download the Cisco AnyConnect VPN client software from Cisco.com and install it on the VPN server.

STEP 2 Download the Cisco IOS version that supports this feature and install it on the VPN server.

STEP 3 Configure SSL VPN on the VPN server.

STEP 4 Ensure the VPN is functional and you can connect to the VPN using the Cisco AnyConnect VPN client.

Configuring the VPN on the Cisco SPA 525G

SPCP Settings (Optional)

If the phone will be connecting to the VPN using SPCP, configure these administrative settings using the web administration interface:

STEP 1 Log in to the web administration interface.

STEP 2 Click the **System** tab.

STEP 3 Under Optional Network Configuration, in the **Alternate TFTP** field, choose **yes**.

STEP 4 In the **TFTP Server** field, enter the IP address of the Cisco Unified Communications 500 Series server. The phone obtains its software load from this server when the phone either boots in SPCP mode (if the **Connect on Bootup** field on the phone is set to **yes**), or connects to the VPN manually (by the user pressing **Connect** on the phone under the **Network Configuration** > **VPN** menu).

STEP 5 Click **Submit All Changes**.

User Settings

Then, enter the user settings for the phone, using either the administration web interface or the phone itself.

To use the web interface:

STEP 1 :Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**. (Not applicable to the SPA 525G in SPCP mode.)

STEP 3 Click the **System** tab.

STEP 4 Under VPN Settings, enter the following:

- In the VPN Server field, enter the IP address of the VPN server.
- In the VPN User Name and Password fields, enter the username and password to log in to the VPN server. These were created when you set up the VPN on the server.
- (Optional) Enter the VPN tunnel group, if required by your VPN server.
- (Optional) To connect to the VPN when the phone is powered on, in the **Connect on Bootup** field, choose **yes**.

STEP 5 Click **Submit All Changes**. If you did not choose **yes** in the **Connect on Bootup** field, connect to the VPN on the phone by pressing the **Setup** button and choosing **Network Configuration** > **VPN** > **Connect**.

To use the phone interface:

STEP 1 On the phone, press the **Setup** button.

STEP 2 Scroll to **Network Configuration** and press **Select**.

STEP 3 Scroll to **Web Server** and ensure that it is enabled. Press the right arrow key if it is not enabled.

STEP 4 Scroll to VPN and press the right arrow key.

STEP 5 Under VPN server, enter the IP address of the VPN server.

STEP 6 Enter the username to log in to the VPN server.

STEP 7 Enter the password for the user.

STEP 8 (Optional) Enter the tunnel group, if required by the VPN server.

STEP 9 (Optional) To connect to the VPN when the phone is powered on, ensure that **Connect on Bootup** is enabled.

STEP 10 To connect to the VPN, ensure that **Connect** is enabled.

STEP 11 Press **Save**. After the VPN connection is established, a VPN icon appears in the upper right of the phone display screen.

To view the VPN status, either:

- Use the web administration interface:
  - Click **Admin Login** and **advanced**. (Not applicable to the SPA 525G in SPCP mode.) Click the **Info** tab.
- Use the phone menu:
  - Press the **Setup** button. Scroll to **Status** and press **Select**. Scroll to **VPN Status** and press **Select**.

6

Provisioning Basics

The Provisioning Tab and its fields are for service provider use only and are not needed in non-SP deployments. This chapter discusses:

VARs and service providers should refer to other documentation, depending on your configuration:

- *Cisco Small Business IP Telephony Devices Provisioning Guide* (service provider login required)
- *Cisco SPA 9000 Voice System Administration Guide*
- Service provider documentation

Provisioning Capabilities

The Cisco IP phones provide for secure provisioning and remote upgrade. Provisioning is achieved through configuration profiles transferred to the device via TFTP, HTTP, or HTTPS.

The Cisco IP phones can be configured to automatically resync their internal configuration state to a remote profile periodically and on power up. The automatic resyncs are controlled by configuring the desired profile URL into the device.

The Cisco IP phones accept profiles in XML format, or alternatively in a proprietary binary format, which is generated by a profile compiler tool, SIP Profile Compiler (SPC), available from Cisco. The Cisco IP phones support up to 256-bit symmetric key encryption of profiles. For the initial transfer of the profile encryption key (initial provisioning stage), the Cisco IP phones can receive a profile from an encrypted channel (HTTPS with client authentication), or can resync to a binary profile generated by the Cisco SIP profile compiler. In the latter case, the SIP profile compiler can encrypt the profile specifically for the target Cisco IP phones, without requiring an explicit key exchange.

Remote firmware upgrade is achieved via TFTP or HTTP or HTTPS (TFTP or HTTP for WIP310). Remote upgrades are controlled by configuring the desired firmware image URL into the Cisco IP phone via a remote profile resync.

Provisioning Configuration from Phone Keypad

Remote provisioning can be performed from a phone keypad. After the user enters the IP address of the provisioning server, the unit resyncs to a known path name. This feature enables service providers to allow VARs to install and provision Cisco phones.

To provision from the phone:

SPA 50XG:

STEP 1 Press **Setup**, then scroll to **Profile Rule**.

STEP 2 Enter the profile rule using the following format, then press the **Resync** soft button.

protocol://server[:port]/profile_pathname

For example:

`tftp://192.168.1.5/spa504.cfg`

If no protocol is specified, TFTP is assumed. If no server-name is specified, the host that requests the URL is used as *server-name*.

If no port is specified, the default port is used (69 for TFTP, 80 for HTTP, and 443 for HTTPS). then the address can be entered in and press **Resync**.

The status of the remote customization process is shown by the phone's mute button blinking in the following patterns:

- Red/orange slow blink (1.0 seconds on, 1.0 seconds off): Contacting server, server not resolvable, not reachable, or down
- Red/orange slow blink (0.2 seconds on, 0.2 seconds off, 0.2 seconds on, 1.4 seconds off): Server responded with file not found or corrupt file

WIP310

STEP 1 Press the **Select** button to choose *Settings* and press the **Select** button again.

STEP 2 Navigate to *Misc Settings*.

STEP 3 Navigate to profile rule. Enter the profile rule in the following format:

protocol://server[:port]/profile_pathname

For example, to have the WIP310 provisioning done by the Cisco SPA 9000 Voice System, enter:

`192.168.2.64/cfg/generic.xml`

SPA 525G

STEP 1 Press the **Setup** button.

STEP 2 Scroll to **Device Administration** and press **Select**.

STEP 3 Scroll to **Profile Rule** and press **Select**.

STEP 4 Enter the profile rule using the following format, then press the **Resync** soft button.

protocol://server[:port]/profile_pathname

For example:

```
tftp://192.168.1.5/spa525.cfg
```

IP Phone Configuration Profiles

The IP phone configuration profile defines the parameter values for a specific device. The configuration profile can be used in two formats:

- Open (XML-style) format
- Proprietary, plain-text format

The XML-style format lets you use standard tools to compile the parameters and values. To protect confidential information contained in the configuration profile, this type of file is generally delivered from the provisioning server to the IP phone over a secure channel provided by HTTPS.

The XML file consists of a series of elements (one per configuration parameter), encapsulated within the element tags <flat-profile> ... </flat-profile>. The encapsulated elements specify values for individual parameters. The following is an example of a valid XML profile:

```
<flat-profile>
<Admin_Passwd>some secret</Admin_Passwd>
<Upgrade_Enable>Yes</Upgrade_Enable>
</flat-profile>
```

The names of parameters in XML profiles can generally be inferred from the Cisco IP phones configuration web pages, by substituting underscores (_) for spaces and other control characters. Further, to distinguish between Lines 1, 2, 3, and 4, corresponding parameter names are augmented by the strings _1_, _2_, _3_, and _4_. For example, Line 1 Proxy is named Proxy_1_ in XML profiles.

The plain-text configuration file uses a proprietary format, which can be encrypted to prevent unauthorized use of confidential information. By convention, the profile is named with the extension .cfg (for example, spa504.cfg). The Cisco SIP Profile Compiler (SPC) tool is provided for compiling the plain-text file containing parameter-value pairs into an encrypted CFG file. The SPC tool is available from Cisco for the Win32 environment (spc.exe) and Linux-i386-elf environment (spc-linux-i386-static). Availability of the SPC tool for the OpenBSD environment is available on a case-by-case basis.

The syntax of the plain-text file accepted by the profile compiler is a series of parameter-value pairs, with the value in double quotes. Each parameter-value pair is followed by a semicolon. The following is an example of a valid text source profile for input to the SPC tool:

```
Admin_Passwd “some secret”;
Upgrade_Enable “Yes”;
```

Parameters in the case of source text files for the SPC tool are similarly named, except that to differentiate Line 1, 2, 3, and 4, the appended strings ([1], [2], [3], or [4]) are used. For example, the Line 1 Proxy is named Proxy[1] in source text profiles for input to the SPC.

Obtaining the SPC Tool

The SPC tool is available on cisco.com. To obtain the software:

STEP 1 Go to:

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=282414147

STEP 2 Click the Profile Compiler (SPC) Tool link.

STEP 3 Choose the version of software that is installed on the phones.

STEP 4 Follow the links to download the software.

General Purpose Parameters

These are configured in the **General Purpose Parameters** section of the **Provisioning** tab. These parameters can be used as variables in provisioning and upgrade rules. They are referenced by prepending the variable name with a '$' character, such as $GPP_A.

You can optionally Require Admin Password to Reset Unit to Factory Defaults (see last line of sample config file).

Sample Configuration File

Following is a sample configuration file:

```
Set_Local_Date_(mm/dd) "" ;
Set_Local_Time_(HH/mm) "" ;
Time_Zone "GMT-07:00" ; # options: GMT-12:00/GMT-11:00/GMT-10:00/GMT-09:00/
GMT-08:00/GMT-07:00/GMT-06:00/GMT-05:00/GMT-04:00/GMT-03:30/GMT-03:00/GMT-
02:00/GMT-01:00/GMT/GMT+01:00/GMT+02:00/GMT+03:00/GMT+03:30/GMT+04:00/
GMT+05:00/GMT+05:30/GMT+05:45/GMT+06:00/GMT+06:30/GMT+07:00/GMT+08:00/
GMT+09:00/GMT+09:30/GMT+10:00/GMT+11:00/GMT+12:00/GMT+13:00
FXS_Port_Impedance "600" ; # options: 600/900/600+2.16uF/900+2.16uF/
270+750||150nF/220+820||120nF/220+820||115nF/370+620||310nF
FXS_Port_Input_Gain "-3" ;
FXS_Port_Output_Gain "-3" ;
DTMF_Playback_Level "-16" ;
DTMF_Playback_Length ".1" ;
Detect_ABCD "Yes" ;
Playback_ABCD "Yes" ;
Caller_ID_Method "Bellcore(N.Amer,China)" ; # options:
Bellcore(N.Amer,China)/DTMF(Finland,Sweden)/DTMF(Denmark)/ETSI DTMF/ETSI
DTMF With PR/ETSI DTMF After Ring/ETSI FSK/ETSI FSK With PR(UK)
FXS_Port_Power_Limit "3" ; # options: 1/2/3/4/5/6/7/8
Protect_IVR_FactoryReset “No” ;
```

NOTE You can optionally require an admin password to reset the phone to factory defaults by setting the last line parameter to "yes."

If you are a service provider with a password, see the *Cisco Small Business IP Telephony Devices Provisioning Guide.*

Upgrading, Resyncing, and Rebooting Phones

Cisco IP phones support secure remote provisioning and firmware upgrades. You can generate configuration profiles using common, open-source tools that integrate with service provider provisioning systems. Supported transport protocols include TFTP, HTTP, and HTTPS with client certificates.

256-bit symmetric key encryption of profiles is supported. In addition, an unprovisioned Cisco IP phone can receive an encrypted profile specifically targeted for that device without requiring an explicit key. a secure first-time provisioning mechanism using SSL functionality.

User intervention is not required to initiate or complete a profile update or firmware upgrade. The Cisco IP phone upgrade logic is capable of automating multi-stage upgrades, if intermediate upgrades are required to reach a future upgrade state from an older release. A profile resync is only attempted when the Cisco IP phone is idle, because this may trigger a software reboot.

General purpose parameters are provided to help service providers manage the provisioning process. Each Cisco IP phone can be configured to periodically contact a normal provisioning server (NPS). Communication with the NPS does not require the use of a secure protocol because the updated profile is encrypted by a shared secret key. The NPS can be a standard TFTP, HTTP or HTTPS server.

The administrator can upgrade, reboot, restart, or resync Cisco IP phones using the web interface. The administrator can also perform these tasks using a SIP notify message and bypassing the web interface.

Upgrading Firmware on a Phone

Use the upgrade URL to upgrade firmware on the Cisco IP phone. You can upgrade from either a TFTP or HTTP server.

The Upgrade Enable parameter on the Provisioning web page must be set to yes:

Cisco IP phone web UI: **Provisioning** > **Firmware Upgrade** > **Upgrade Enable: yes**

Use the following syntax to upgrade firmware on a phone:

```
http://phone-ip-address/admin/upgrade?protocol://server-
name[:port]]/firmware-path
```

- Protocol defaults to TFTP.
- Server name is the host requesting the URL.

- Port is the port of the protocol being used (for example, 69 for TFTP or 80 for HTTP).
- F*irmware-path* defaults to /spa.bin (for example, http://192.168.2.217/admin/upgrade?tftp://192.168.2.251/spa.bin) for SPA phones and /wip310.img for the WIP310. The firmware-pathname is typically the file name of the binary located in a directory on the TFTP or HTTP server.

Firmware Upgrade Parameters

The following table defines the function and usage of each parameter in the Firmware Upgrade section of the *Provisioning* tab.

Parameter	Description
Upgrade_Enable	Enables firmware upgrade operations independently of resync actions. Defaults to Yes.
Upgrade_Error_Retry_Delay	The upgrade retry interval (in seconds) applied in case of upgrade failure. The device has a firmware upgrade error timer that activates after a failed firmware upgrade attempt. The timer is initialized with the value in this parameter. The next firmware upgrade attempt occurs when this timer counts down to zero. The default is 3600 seconds.
Downgrade_Rev_Limit	Enforces a lower limit on the acceptable version number during a firmware upgrade or downgrade. The device does not complete a firmware upgrade operation unless the firmware version is greater than or equal to this parameter. The default is (empty).
Upgrade_Rule	This parameter is a firmware upgrade script with the same syntax as Profile_Rule. Defines upgrade conditions and associated firmware URLs. The default is (empty).
Log_Upgrade_Request_Msg	Syslog message issued at the start of a firmware upgrade attempt. The default is $PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH

Parameter	Description
Log_Upgrade_Success_Msg	Syslog message issued after a firmware upgrade attempt completes successfully. The default is $PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR
Log_Upgrade_Failure_Msg	Syslog message issued after a failed firmware upgrade attempt. The default is $PN $MAC -- Upgrade failed: $ERR.
License Keys	This field is empty.

Resyncing a Phone

You can resync an IP phone to a specific remote profile. The configuration of the phone you resync will match the configuration of the remote phone. The phone can be configured to resync its internal configuration state to a remote profile periodically and on power up.

NOTE The phone resyncs only when it is idle.

Use the following syntax to resync a phone's profile to a profile on a TFTP, HTTP, or HTTPS server:

`http://phone-ip-addr/admin/resync?protocol://server-name[:port]/profile-pathname`

- Parameter following resync? defaults to the Profile Rule setting on the web server Provisioning page.
- Protocol defaults to TFTP.
- Server-name defaults to the host requesting the URL.

- Port defaults to:
  - 69 for TFTP
  - 80 for HTTP
  - 443 for HTTPS
- Profile-*path* defaults to the path to the new resync profile (for example, http://192.168.2.217admin/resync?tftp://192.168.2.251/spaconf.cfg).

Rebooting a Phone

You can remotely reboot a Cisco IP phone if needed.

Use the following syntax to reboot a phone:

`http://phone-ip-address/admin/reboot`

Redundant Provisioning Servers

The provisioning server may be specified as an IP address or as a fully qualified domain name (FQDN). The use of a FQDN facilitates the deployment of redundant provisioning servers. When the provisioning server is identified through a FQDN, the Cisco IP phone attempts to resolve the FQDN to an IP address through DNS. Only DNS A-records are supported for provisioning; DNS SRV address resolution is not available for provisioning. The Cisco IP phone continues to process A-records until the first server responds. If no server associated with the A-records responds, the Cisco IP phone logs an error to the syslog server.

Retail Provisioning

The Cisco IP phone includes an web UI that displays internal configuration and accepts new configuration parameter values. The server also accepts a special URL command syntax for performing remote profile resync and firmware upgrade operations.

In a retail distribution model, a customer purchases a Cisco voice endpoint device, and subsequently subscribes to a particular service. The customer first signs on to the service and establishes a VoIP account, possibly through an online portal. Subsequently, the customer binds the particular device to the assigned service account.

To do so, the unprovisioned Cisco IP phone is instructed to resync with a specific provisioning server through a resync URL command. The URL command typically includes an account PIN number or alphanumeric code to associate the device with the new account.

In the following example, a device at the DHCP-assigned IP address 192.168.1.102 is instructed to provision itself to the SuperVoIP service:

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/cisco-init/
1234abcd
```

In this example, 1234abcd is the PIN number of the new account. The remote provisioning server is configured to associate the Cisco IP phone that is performing the resync request with the new account, based on the URL and the supplied PIN. Through this initial resync operation, the Cisco IP phone is configured in a single step, and is automatically directed to resync thereafter to a permanent URL on the server. For example:

```
https://prov.supervoip.com/cisco-init
```

For both initial and permanent access, the provisioning server relies on the Cisco IP phone client certificate for authentication and supplies correct configuration parameter values based on the associated service account.

Automatic In-House Preprovisioning

Using the web UI and issuing a resync URL is convenient for a customer in the retail deployment model, but it is not as convenient for preprovisioning a large number of units.

The Cisco IP phone supports a more convenient mechanism for in-house preprovisioning. With the factory default configuration, a Cisco IP phone automatically tries to resync to a specific file on a TFTP server, whose IP address is offered as one of the DHCP-provided parameters. This lets a service provider connect each new Cisco IP phone to a LAN environment configured to

preprovision phones. Any new Cisco IP phone connected to this LAN automatically resyncs to the local TFTP server, initializing its internal state in preparation for deployment. Among other parameters, this preprovisioning step configures the URL of the Cisco IP phone provisioning server.

Subsequently, when a new customer signs up for service, the preprovisioned Cisco IP phone can be simply bar-code scanned, to record its MAC address or serial number, before being shipped to the customer. Upon receiving the unit, the customer connects the unit to the broadband link. On power-up the Cisco IP phone already knows the server to contact for its periodic resync update.

Configuration Access Control

Besides configuration parameters that control resync and upgrade behavior, the Cisco IP phone provides mechanisms for restricting end-user access to various parameters.

The Cisco IP phone firmware provides specific privileges for login to a User account and an Admin account. The Admin account is designed to give the service provider or VAR configuration access to the Cisco IP phone, while the User account is designed to give limited and configurable control to the end user of the device.

The User and Admin accounts can be independently password protected. The configuration parameters available to the User account are completely configurable in the Cisco IP phone, on a parameter-by-parameter basis. Optionally, user access to the Cisco IP phone web UI can be totally disabled.

The Internet domains accessed by the Cisco IP phone for resync, upgrades, and SIP registration for Line 1 can be restricted.

Using HTTPS

The Cisco IP phone provides a reliable and secure provisioning strategy based on HTTPS requests from the Cisco IP phone to the provisioning server, using both server and client certificates for authenticating the client to the server and the server to the client.

To use HTTPS with Cisco IP phones, you must generate a Certificate Signing Request (CSR) and submit it to Cisco. The Cisco IP phone generates a certificate for installation on the provisioning server that is accepted by Cisco IP phones when they seek to establish an HTTPS connection with the provisioning server.

The Cisco IP phone implements up to 256-bit symmetric encryption, using the American Encryption Standard (AES), in addition to 128-bit RC4. The Cisco IP phone supports the Rivest, Shamir, and Adelman (RSA) algorithm for public/private key cryptography.

Server Certificates

Each secure provisioning server is issued an secure sockets layer (SSL) server certificate, directly signed by Cisco. The firmware running on the Cisco IP phone clients recognizes only these certificates as valid. The clients try to authenticate the server certificate when connecting via HTTPS, and reject any server certificate not signed by Cisco.

This mechanism protects the service provider from unauthorized access to the Cisco IP phone endpoint, or any attempt to spoof the provisioning server. This might allow the attacker to reprovision the Cisco IP phone to gain configuration information, or to use a different VoIP service. Without the private key corresponding to a valid server certificate, the attacker is unable to establish communication with a Cisco IP phone.

Client Certificates

In addition to a direct attack on the Cisco IP phone, an attacker might attempt to contact a provisioning server using a standard web browser, or other HTTPS client, to obtain the Cisco IP phone configuration profile from the provisioning server. To prevent this kind of attack, each Cisco IP phone also carries a unique client certificate, also signed by Cisco, including identifying information about each individual endpoint. A certificate authority root certificate capable of authenticating the device client certificate is given to each service provider. This authentication path allows the provisioning server to reject unauthorized requests for configuration profiles.

Obtaining a Server Certificate

To obtain a server certificate:

STEP 1 Contact a Cisco support person who will work with you on the certificate process. If you are not working with a specific support person, you can email your request to *linksys-certadmin@cisco.com*.)

STEP 2 Generate a private key that will be used in a CSR (Certificate Signing Request). This key is private and you do not need to provide this key to Cisco support. Use open source "openssl" to generate the key. For example:

```
openssl genrsa -out <file.key> 1024
```

STEP 3 Generate CSR a that contains fields that identify your organization, and location. For example:

```
openssl req -new -key <file.key> -out <file.csr>
```

You must have the following information:

- Subject field—Enter the Common Name (CN) that must be a FQDN (Fully Qualified Domain Name) syntax. During SSL authentication handshake, the SPA 9000 verifies that the certificate it receives is from the machine that presented it.
- Server's hostname—For example, provserv.domain.com.
- Email address—Enter an email address so that customer support can contact you if needed. This email address is visible in the CSR.

STEP 4 Email the CSR (in zip file format) to the Cisco support person or to *linksys-itsp@external.cisco.com*. The certificate is signed by Cisco and given to you.

7

Configuring Regional Parameters and Supplementary Services

Use the *Regional* tab to configure regional and local settings, such as Vertical Service Activation codes (star codes), Vertical Service Announcement Codes, and local language and dictionary. See the following sections:

Cisco IP phones have configurable call progress tones. Parameters for each type of tone can include number of frequency components, frequency and amplitude of each component, and cadence information.

The call progress tone pass-through feature lets you hear call progress tones (such as ringing) that are generated from the far-end network.

Advanced Scripting for Cadences, Call Progress Tones, and Ring Tones

Advanced information on defining tones an and cadences follows.

A CadScript is a mini-script that specifies the cadence parameters of a signal. It can be up to 127 characters. The syntax follows:

1[;S2]—where Si=Di(oni,1/offi,1[,oni,2/offi,2[,oni,3/offi,3[,oni,4/offi,4[,oni,5/offi,5[,oni,6/offi,6]]]]]) and is known as a *section*, oni,j and offi,j are the on/off duration in seconds of a *segment* and i = 1 or 2, and j = 1 to 6.

Di is the total duration of the section in seconds. All durations can have up to 3 decimal places to provide 1 ms resolution. The wildcard character "*" stands for infinite duration. The segments within a section are played in order and repeated until the total duration is played.

Example 1: Normal Ring

```
60(2/4)
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60 s
Number of Segments = 1
Segment 1: On=2s, Off=4s
Total Ring Length = 60s
```

Example 2: Distinctive Ring (short,short,short,long)

```
60(.2/.2,.2/.2,.2/.2,1/4)
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60s
Number of Segments = 4
Segment 1: On=0.2s, Off=0.2s
Segment 2: On=0.2s, Off=0.2s
Segment 3: On=0.2s, Off=0.2s
Segment 4: On=1.0s, Off=4.0s
Total Ring Length=60s
```

A ToneScript is a mini-script that specifies the frequency, level and cadence parameters of a call progress tone. It can contain up to 127 characters. The syntax follows:

FreqScript;Z1[;Z2]. The section Zi is similar to the Si section in a CadScript except that each on/off segment is followed by a frequency components parameter: Zi = Di(oni,1/offi,1/fi,1[,oni,2/offi,2/fi,2 [,oni,3/offi,3/fi,3 [,oni,4/offi,4/fi,4 [,oni,5/offi,5/fi,5 [,oni,6/offi,6/fi,6]]]]])

where fi,j = n1[+n2]+n3[+n4[+n5[+n6]]]] and 1 < nk < 6 indicates which of the frequency components given in the FreqScript are used in that segment; if more than one frequency component is used in a segment, the components are summed together.

Example 1: Dial Tone

```
350@-19,440@-19;10(*/0/1+2)
Number of Frequencies = 2
Frequency 1 = 350 Hz at –19 dBm
Frequency 2 = 440 Hz at –19 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 10 s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2
Total Tone Length = 10s
Example 2: Stutter Tone
350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)
Number of Frequencies = 2
Frequency 1 = 350 Hz at –19 dBm
Frequency 2 = 440 Hz at –19 dBm
Number of Cadence Sections = 2
Cadence Section 1: Section Length = 2s
Number of Segments = 1
Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
Cadence Section 2: Section Length = 10s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2
Total Tone Length = 12s
```

Example 3: SIT Tone

```
985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0)
Number of Frequencies = 3
Frequency 1 = 985 Hz at –16 dBm
Frequency 2 = 1428 Hz at –16 dBm
Frequency 3 = 1777 Hz at –16 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 20s
Number of Segments = 4
Segment 1: On=0.38s, Off=0s, with Frequency 1
Segment 2: On=0.38s, Off=0s, with Frequency 2
Segment 3: On=0.38s, Off=0s, with Frequency 3
Segment 4: On=0s, Off=4s, with no frequency components
Total Tone Length = 20s
```

A RingScript is a mini-script that describes a ring tone. The syntax follows:

n=*ring-tone-name*;w=*waveform-id-or-path*;c=*cadence-id*;b=*break-time*;t=*total-time*

ring-tone-name is a name to identify this ring tone specification. This name will appear on the Ring Tone menu of the phone. The same name can be used in a SIP Alert-Info header in an inbound INVITE request to tell the phone to play the corresponding ring tone specification. Because of this, the name should contain characters allowed in a URL only.

Waveform-id is the index of the desired waveform to use in this ring tone specification. There are 4 built-in waveforms:

- 1 = A classic phone with mechanical bell
- 2 = Typical phone ring
- 3 = A classic ring tone
- 4 = A wide-band frequency sweep signal

This field can also be a network path (url) to download a ring tone data file from a server on-the-fly. In this case, the syntax of the field is

w=[tftp://]hostname[:port]/path.

cadence-id is the index of the desired cadence to play the given waveform. 8 cadences (1–8) as defined in <Cadence 1> through <Cadence 8>. *Cadence-id* can be 0 If w=3,4, or an url. Setting c=0 implies the on-time is the natural length of the ring tone file.

break-time specifies the number of seconds to break between two bursts of ring tone, such as b=2.5

total-time specifies the total number of seconds to play the ring tone before it times out

Example 1: SIT Tone

```
n=Classic-1,w=3;c=1
n=Simple-1,w=2;c=1
```

Call Progress Tones

For definitions of all call progress tones, see **"Call Progress Tones" section on page 226**.

Distinctive Ring Patterns

Ring cadence defines the ringing pattern that announces a telephone call.

NOTE The WIP310 has only eight distinctive ring pattern fields.

The pattern is:

`length(on/off)`

where:

- Length: The total length of the ring
- On: The number of "on" seconds
- Off: The number of "off" seconds.

Example 1: Normal Ring

`60(2/4)`

- Number of Cadence Sections = 1
- Cadence Section 1: Section Length = 60 s
- Number of Segments = 1
- Segment 1: On=2s, Off=4s
- Total Ring Length = 60s

Example 2: Distinctive Ring (short,short,short,long)

`60(.2/.2,.2/.2,.2/.2,1/4)`

- Number of Cadence Sections = 1
- Cadence Section 1: Section Length = 60s

- Number of Segments = 4
- Segment 1: On=0.2s, Off=0.2s
- Segment 2: On=0.2s, Off=0.2s
- Segment 3: On=0.2s, Off=0.2s
- Segment 4: On=1.0s, Off=4.0s
- Total Ring Length=60s

Control Timer Values (sec)

The following table describes all control timer parameters. Each value is displayed in seconds.

Field	Description
Reorder Delay	Delay after far end hangs up before reorder tone is played. 0 = plays immediately, inf = never plays. Range: 0–255 seconds. Defaults to 5.
Call Back Expires	Expiration time in seconds of a call back activation. Range: 0–65535 seconds. Defaults to 1800.
Call Back Retry Intvl	Call back retry interval in seconds. Range: 0–255 seconds. Defaults to 30.
Call Back Delay	Delay after receiving the first SIP 18x response before declaring the remote end is ringing. If a busy response is received during this time, the Cisco IP phone still considers the call as failed and keeps on retrying. Defaults to 0.5.

Field	Description
Interdigit Long Timer	Long timeout between entering digits when dialing. The interdigit timer values are used as defaults when dialing. The *Interdigit Long Timer* is used after any one digit, if all valid matching sequences in the dial plan are incomplete as dialed. Range: 0–64 seconds. Setting this value high can result in a longer post dialing delay (PDD), which is the time between the start of a call and the time the phone starts ringing. A value that is too low can result in dialed digits not being correctly recognized. Defaults to 10.
Interdigit Short Timer	Short timeout between entering digits when dialing. The *Interdigit Short Timer* is used after any one digit, if at least one matching sequence is complete as dialed, but more dialed digits would match other as yet incomplete sequences. Range: 0–64 seconds. Defaults to 3.

Configuring Supplementary Services (Star Codes)

The Cisco IP phones provide native support of a large set of enhanced or supplementary services (also known as star codes). A user can enter star codes (such as *21 for call forward, followed by the target number) to perform call features such as call return, blind call transfers, call pickup, and so on. These codes can be handled locally by the phone or to be sent to the network as an INVITE to the service provider.

NOTE Some service providers choose to disable star codes. See **"Configuring Supplementary Services (Star Codes)" section on page 153**.

Entering Star Code Values

The phone provides default values for star codes. You can change the default star code values for your area or region.

To configure star code values:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Regional** tab.

STEP 4 Under **Vertical Service Activation Codes**, enter the values you want to change for the codes.

STEP 5 Click **Submit All Changes**.

The codes are as follows:

- Call Return (*69)—Calls the last caller, regardless which extension.
- Blind Transfer (*98)—Allows the user to transfer a call to another number without waiting for the other party to pick up.
- Call Back Act (*66)—Periodically redials the last busy number (every 30 seconds by default) until it rings or until the attempt expires (30 min by default), regardless which extension. Only one call back operation can be ordered at a time. A new order automatically cancels the previous order.
- Call Back Deact (*86)—Cancels the last call back operation.
- Call Forward All Act (*72)—Call forwards all inbound calls. Applies to primary extension only.
- Call Forward All Deact (*73)—Cancels call forward all. Applies to primary extension only.
- Call Forward Busy Act (*90)—Call forwards on busy. Applies to primary extension only.
- Call Forward Busy Deact (*91)—Cancels call forward on busy. Applies to primary extension only.
- Call Forward No Answer Act (*92)—Call forwards if no answer. Applies to primary extension only.
- Call Forward No Answer Deact (*93)—Cancels call forward no answer. Applies to primary extension only.

- CW Act (*56)—Enables call waiting. For example, if call waiting is turned off globally, this star code will turn on call waiting until the CW Deact code is entered.
- CW Deact (*57)—Deactivates call waiting. For example, if call waiting is turned on globally, this star code deactivates call waiting until the CW Act code is entered.
- CW Per Call Act (*71)—Enables call waiting for a single call. For example, if call waiting is turned off globally, this star code will turn on call waiting for that call.
- CW Per Call Deact (*70)—Deactivates call waiting for a single call. For example, if call waiting is turned on globally, this star code deactivates call waiting for that call.
- Block CID Act (*67)—Blocks caller ID on all outbound calls. Applies to all extensions.
- Block CID Deact (*68)—Deactivates caller ID blocking on outbound calls. Applies to all extensions.
- Block CID Per Call (*81)—Blocks caller ID on the next outbound call (on the current call appearance only).
- Block CID Per Call Deact (*82)—Deactivates caller ID blocking on the next outbound call (on the current call appearance only).
- Block ANC Act—Blocks anonymous calls. Applies to all extensions.
- Block ANC Deact—Deactivates anonymous call blocking. Applies to all extensions.
- DND Act (*78)—Activates Do Not Disturb. Applies to all extensions.
- DND Deact (*79)—Deactivates Do Not Disturb. Applies to all extensions.
- Secure All Call Act (*16)—Defaults to prefer to use encrypted media (voice codecs).
- Secure No Call Act (*17)—Defaults to prefer to use unencrypted media for all outbound calls. Applies to all extensions.
- Secure One Call Act (*18)—Prefers to use encrypted media for the outbound call (on this call appearance only).
- Secure One Call Deact (*19)—Prefers to use unencrypted media for the outbound call (on this call appearance only).

- Paging (*96)—Pages the number called.
- Call Park (*38)—Parks a call on an entered line number.
- Call UnPark Code (*39)—Retrieves a call from an entered line number.
- Call Pickup (*36)—Picks up a call at an entered extension.
- Group Call Pickup (*37)—Picks up a ringing call at a group of extensions.
- Media Loopback Code (*03)—A service provider can set up a test call from an IP media loopback server (the source) to a subscriber's VoIP device (the mirror). The test call provides statistical reporting on network performance and audio quality.

  Depending on the source's capabilities, the SP can see packet jitter, loss, and delay (although Media Loopback cannot identify an offending hop). This helps the SP identify an offending hop that could be causing issues in VoIP calls to a subscriber. The test results can also provide audio quality scoring, which lets a SP better understand the subscriber's experience.
- Referral Services Codes—One or more * codes can be configured into this parameter, such as *98, or *97|*98|*123, and so on. The maximum total length is 79 characters.

  This parameter applies when the user places the current call on hold (by Hook Flash) and is listening to second dial tone. Each * code (and the following valid target number according to current dial plan) entered on the second dial-tone triggers the Cisco IP phone to perform a blind transfer to a target number that is prepended by the service * code. For example:

a. After the user dials *98, the Cisco IP phone plays a special prompt tone while waiting for the user the enter a target number (which is validated according to the dial plan as in normal dialing).

b. When a complete number is entered, the Cisco IP phone sends a blind REFER to the holding party with the Refer-To target equals to *98 *target_number.* This feature allows the Cisco IP phone to hand off a call to an application server to perform further processing, such as call park.

The * codes should not conflict with any of the other vertical service codes internally processed by the Cisco IP phone. You can delete any * code that you do not want to SPA9000 to process.

Feature Dial Services Codes: Tells the Cisco IP phone what to do when the user is listening to the first or second dial tone.

You can configure one or more * codes into this parameter, such as *72, or *72|*74|*67|*82, and so on. The maximum total length is 79 characters. When the user has a dial tone (first or second dial tone), they can enter a * code (and the following target number according to current dial plan) to trigger the Cisco IP phone to call the target number prepended by the * code. For example:

a. After the user dials *72, the Cisco IP phone plays a special prompt tone while waiting for the user the enter a target number (which is validated according to the dial plan as in normal dialing).

b. When a complete number is entered, the Cisco IP phone sends an INVITE to *72 *target_number* as in a normal call. This feature allows the proxy to process features such as call forward (*72) or BLock Caller ID (*67).

You can add a parameter to each * code in *Features Dial Services Codes* to indicate what tone to play after the * code is entered, such as *72‘c’|*67‘p‘. Following is a list of allowed dial tone parameters (note the use of back quotes surrounding the parameter without spaces).

- ‘c‘ = Cfwd dial tone
- ‘d‘ = Dial tone
- ‘m‘ = MWI dial tone
- ‘o‘ = Outside dial tone
- ‘p‘ = Prompt dial tone
- ‘s‘ = Second dial tone
- ‘x‘ = No tones are place, x is any digit not used above

If no tone parameter is specified, the Cisco IP phone plays the prompt tone by default.

If the * code is not to be followed by a phone number, such as *73 to cancel call forwarding, do not include it in this parameter. In that case, add that * code in the dial plan.

Activating or Deactivating Supplementary Services

You can disable services handled locally by the phone in one of two ways:

- Delete the star code in the *Vertical Service Activation* section in the **Regional** tab.
- Disable the service in the ***Phone*** tab. See **Configuring Supplementary Services (Star Codes), page 153**.

NOTE If a service is enabled in the Phone tab but cleared in the Regional tab, the service can still be enabled/disabled by the end- user from the phone LCD or the web UI. If a service is disabled, the soft button associated with that service is hidden on the LCD. Also, any menu item associated with a disabled service is preceded with an exclamation mark (!).

A supplementary service should be disabled if

- the user has not subscribed for it

or

- the service provider intends to support similar service using other means than relying on the Cisco IP phone.

Vertical Service Announcement Codes (SPA 500 Series)

The SPA 500 Series IP phones support all services that can be activated on a phone (call forward, do not disturb, and so on). Vertical service announcement codes apply only when the user dials the corresponding star code.

Following is an example of how you can use these fields:

```
<Service Annc Base Number> = 1234
<Service Annc Extension Codes>=
"CWT:00;CWF:01;FAT:02;FAF:05;FBT:03;FBF:05;FNT:04;FNF:05;"
Here CWT: Call waiting service enabled;
CWF: Call waiting service disabled;
FAT: Call forward all service enabled;
FAF: Call forward all service disabled;
FBT: Call forward busy service enabled;
FBF: Call forward busy service disabled;
FNT: Call forward no answer enabled;
FNF: Call forward no answer disabled;
```

When the user enables call waiting service, the IP phone automatically calls "1234*00*@$proxy".

When the user *disables* the call waiting service, IP phone connects to "1234*01*@$proxy".

If the <Service Annc Extension Codes> do not define CWT/CWF extension codes, the IP phone defaults to normal.

Bonus Services Announcement description

When the user enables the callback service using the *code, the IP phone automatically calls “123400@$proxy.”

When the user disables the callback service using the *code, the IP phone automatically connects to the “123401@$proxy.”

If the *Service Annc Extension Codes* do not define CBT/CBF extension codes, the IP phone does not use this feature.

```
[Line1/2]<Service Announcement Serv> = Yes
[Regional]<Service Annc Base Number> = {announcement server base number}
[Regional]<Service Annc Extension Codes> = {SAEC Script}
SAEC Script format:{SA_map;}*    Here * means 0 or multiple
SA_map syntax:
      SA_serv=SA_extcode
      SA_serv is the name of service plus the current condition;
      SA_extcode is the extension code which the ANNC server will route to.
Appendix: SA_serv list
    1) Call Back
    CBT: Call back enabled
    CBF: Call back disabled
    CBB: Call back busy enabled
2) Call Forward
    FAT: Call forward all enabled
    FAF: Call forward all disabled
    FBT: Call forward busy enabled
    FBF: Call forward busy disabled
    FNT: Call forward no answer enabled
    FNF: Call forward no answer disabled
    FLT: Call forward last enabled
    FLF: Call forward last disabled
3) Call Waiting
    CWT: Call waiting enabled
    CWF: Call waiting disabled
4) Block Last Call
    BLT: Block last call enabled
    BLF: Block last call disabled
5) Accept Last Call
    ALT: Accept last call enabled
    ALF: Accept last call disabled
```

```
6) Block Caller ID
    BCT: Block caller id enabled
    BCF: Block caller id disabled
7) Distinctive Ringing
    DRT: Distinctive ringing enabled
    DRF: Distinctive ringing disabled
8) Speed Dial
    SDT: Speed dial enabled
    SDF: Speed dial disabled
9) Secure Call
    SCT: Secure call enabled
    SCF: Secure call disabled
10) Do Not Disturb
    DDT: DND enabled
    DDF: DND disabled
11) Caller ID
    CDT: Caller ID enabled
    CDF: Caller ID disabled
12) CW CID
    WDT: CWCID enabled
    WDF: CWCID disabled
13) Block Anonymous call
    BAT: Block anonymous call enabled
    BAF: Block anonymous call disabled
```

Outbound Call Codec Selection Codes

Codec call selection codes affect voice quality. For more information about voice codecs, see the **"Supported Codecs" section on page 114**.

- You can choose a *preferred* codec for a call or *force* a call to use a specific codec.
- *Prefer G.711u (*017110)* through *G.729a (*01729)*—Sets the preferred codec for next outbound call. If the preferred codec is unavailable, the second, then the third preferred codec is used, if specified (see the **"Configuring Voice Codecs" section on page 119**).
- Force *G.711u (*027110)* through *G.729a (*02729)* —Forces the specified codec for next outbound call. If the specified codec is unavailable, the preferred codecs are used in order, if specified (see the **"Configuring Voice Codecs" section on page 119**).

Miscellaneous Parameters

This section contains both DTMF parameters and localization parameters:

DTMF Parameters

Dual Tone Multi-Frequency (DTMF) is the system used by touch-tone phones. DTMF assigns a specific frequency (consisting of two separate tones) to each key so that it can easily be identified by a microprocessor.

In-Band and Out-of-Band (RFC 2833): IP phones can relay DTMF digits as out-of-band events to preserve the fidelity of the digits. This can enhance the reliability of DTMF transmission required by many IVR applications such as dial-up banking and airline information.

The following parameters can either help false detection or get better detection by the IVR. In general, the default values are recommended for both IVR functions.

- *DTMF Playback Level*: Local DTMF playback level in decibels per minute, up to one decimal place. Applicable locally when a user presses a digit or when the phone receives an out-of-band (OOB) DTMF signal from the network side. Does not affect DTMF transmission. Defaults to -16.
- *DTMF Playback Length*: Local DTMF playback duration in milliseconds. Affects only OOB. Defaults to .1.
- *Inband DTMF Boost*: Controls the amount of amplification applied to DTMF signals. Affects only tones sent by inband method. Choices are 0, 3, 6, 9, 12, 15, and 18 decibels. Defaults to 12 dB.

To help false detection, avoid inband and use OOB. With OOB, the DTMF Playback Length does not matter. If you use inband, use a smaller DTMF Boost value.

To get better detection by the IVR, avoid inband and use OOB. This way, the DTMF tone is reconstructed by the PSTN gateway or the remote endpoint, and the quality is not subject to distortion from the audio codec. If you use OOB, use a slightly longer DTMF Playback Length.

If you use inband, use a higher Inband DTMF boost.

Localizing Your IP Phone

The following table describes the localization parameters in the *Miscellaneous* section.

Field	Description
Set Local Date (mm/dd)	Enter the local date (*mm* represents the month and *dd* represents the day). The year is optional and uses two or four digits. For example, May 1, 2008, can be entered as: **05/01** or **05/01/08** or **05/01/2008**
Set Local Time (HH/mm)	Enter the local time (*hh* represents hours and *mm* represents minutes). Seconds are optional.
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00,..., GMT, GMT+01:00, GMT+02:00, ..., GMT+13:00. Defaults to GMT-08:00.
Time Offset (HH/mm)	This specifies the offset from GMT to use for the local system time.
Daylight Saving Time Rule	Enter the rule for calculating daylight saving time. See the **"Configuring Daylight Savings Time" section on page 164**.
Daylight Saving Enable	Select **yes** to enable or **no** to disable DST on the phone. This setting affects all lines (extensions) on the phone.
Dictionary Server Script	Defines the location of the dictionary server, the languages available and the associated dictionary. See the **"Creating a Dictionary Server Script" section on page 167**.

Field	Description
Language Selection	Specifies the default language. The value must match one of the languages supported by the dictionary server. The script (dx value) is as follows: <Language_Selection ua="na"> </Language_Selection> Defaults to blank; the maximum number of characters is 512. For example: <Language_Selection ua="na"> Spanish </Language_Selection>

Managing the Time and Date

Cisco IP phones obtain the current time information in one of three ways:

- NTP Server—You can configure one or two NTP servers on the phone. When the phone first boots up, it tries to contact the first NTP server to get the current time. The phone periodically synchronizes its time with the NTP server. The synchronization period is fixed at 1 hour. In between updates, the phone tracks time with its own internal clock.
- SIP Messages—Each SIP message (request or response) sent to the phone may contain a Date header with the current time information. If the header is present, the phone uses it to update its current time.
- Manual Setup—The phone also lets you manually enter the current time and date from the phone GUI or the web UI. However, this value is overridden by the NTP time or SIP Message Date whenever they are available to the phone. Manual setup requires you to enter the time in 24-hour format only.

The time served by the NTP Server and the SIP Date Header are expressed in GMT time. The local time is obtained by offsetting the GMT according to the time zone of the region.

The *Time Zone* parameter can be configured from the web page or through provisioning. This time can be further offset by the *Time Offset (HH/mm)* parameter, which must be entered in 24-hour format. This parameter can also be configured from the phone's LCD display.

NOTE The *Time Zone* and *Time Offset (HH/mm)* offset values are *not* applied to manual time and date setup.

Configuring Daylight Savings Time

The phone supports auto adjustment for daylight saving time. You must set *Daylight Savings Time Enable* to **yes** and enter the DST rule. This option affects the time stamp on *CallerID*.

To enter the rule for calculating DST, include the start, end, and save values separated by semi-colons (;) as follows:

`Start = start-time; end=end-time; save = save-time`

For example, the default DST rule is

`start=4/1/7;end=10/-1/7;save=1.`

The *start-time* and *end-time* values specify the start and end dates and times of daylight saving time. Each value is in this format: *month/day/ weekday[/HH:mm:ss]*

The *month* value equals any value in the range 1-12 (January-December).

The *day* value equals any + or - value in the range 1-31. If day is 1, it means the weekday on or before the end of the month (in other words the last occurrence of weekday in that month).

The *weekday* value equals any value in the range 1-7 (Monday-Sunday). It can also equal 0. If the weekday value is 0, this means that the date to start or end daylight saving is exactly the date given. In that case, the day value must not be negative. If the weekday value is not 0 and the day value is positive, then daylight saving starts or ends on the weekday value on or after the date given. If the weekday value is not 0 and the day value is negative, then daylight saving starts or ends on the weekday value on or before the date given.

Optional time values: *HH* represents hours (0-23), *mm* represents minutes (0-59). and *ss* represents seconds (0-59). Optional values inside brackets [ ] are assumed to be 0 if not specified. Midnight is represented by 0:0:0 of the given date.

The *save-time* value is the number of hours, minutes, and/or seconds to add to the current time during DST. The *save-time* value can be preceded by a plus (+) or minus (-) sign to indicate addition or subtraction.

Daylight Saving Time Examples

The following example configures daylight savings time for the U.S, adding one hour starting at midnight on the first Sunday in April and ending at midnight on the last Sunday of October; add 1 hour (USA, North America):

```
start=4/1/7/0:0:0;end=10/31/7/0:0:0;save=1
start=4/1/7;end=10/-1/7;save=1
start=4/1/7/0;end=10/-1/7/0;save=1
```

The following example configures daylight savings time for Egypt, starting at midnight on the last Sunday in April and ending at midnight on the last Sunday of September:

```
start=4/-1/7;end=9/-1/7;save=1 (Egypt)
```

The following example configures daylight savings time for New Zealand, starting at midnight on the first Sunday of October and ending at midnight on the third Sunday of March. This only applies to countries that recognize daylight savings time.

```
start=10/1/7;3/22/7;save=1 (New Zealand)
```

The following example reflects the new change starting March 2007. DST starts on the second Sunday in March and ends on the first Sunday in November:

```
start=3/8/7/02:0:0;end=11/1/7/02:0:0;save=1
```

Selecting a Display Language

This section describes how to localize the SPA 500 Series IP Phone display language. You can define up to nine languages, in addition to English, to be available and host the dictionaries for each of the languages on the HTTP or TFTP provisioning server. Language support follows Cisco dictionary principles.

NOTE The WIP310 does not support localization; however, daylight savings time adjustment is supported.

Use the Language Selection parameter to select the phone's default display language. The value must match one of the languages supported by the dictionary server. The script (dx value) is as follows:

- <Language_Selection ua="na">
- </Language_Selection>

Defaults to blank; the maximum number of characters is 512. For example:

```
<Language_Selection ua="na"> Spanish
</Language_Selection>
```

During startup, the phone checks the selected language and downloads the dictionary from the TFTP/HFTP provisioning server indicated in the phone's configuration. The dictionaries are available at the support website. See **Appendix C, "Where to Go From Here,"** for the website location.

Currently dictionaries are available for the following languages:

- English
- Spanish
- German
- Dutch
- Italian
- French
- Portuguese
- Danish
- Swedish
- Czech
- Slovak

NOTE For language selection, the following character sets are supported: Latin2 (Czech, Hungarian, Polish, Romanian, Croatian, Slovak, Slovenian, Serbian), Cyrillic (Russian, Bulgarian, Ukrainian and others), and Latin5 (Turkish).
The phones officially support the ISO-8859-1 to 8859-16 character sets, which encompass all Eastern and Western European languages.

The end user can change the language of the phone on the phone by following these steps:

STEP 1 Press the **Setup** button.

STEP 2 Select **Language**, then press the **Select** soft button.

STEP 3 Select **Option** to change the language.

STEP 4 With the desired language selected, press **Save**.

Creating a Dictionary Server Script

The Dictionary Server Script defines the location of the dictionary server, the languages available and the associated dictionary. The syntax is as follows:

```
Dictionary_Server_Script ua="na"/Dictionary_Server_Script
```

Defaults to blank; the maximum number of characters is 512. The detailed format is as follows:

```
serv={server ip port and root path};
d0=language0;x0=dictionary0 filename;
d1=language1;x1=dictionary1 filename;
d2=language2;x2=dictionary2 filename;
d3=language3;x3=dictionary3 filename;
d4=language4;x4=dictionary4 filename;
d5=language5;x5=dictionary5 filename;
d6=language6;x6=dictionary6 filename;
d7=language3;x7=dictionary7 filename;
d8=language8;x8=dictionary8 filename;
d9=language5;x9=dictionary9 filename;
```

For example:

```
Dictionary_Server_Script ua="na"
serv=tftp://192.168.1.119/
;d0=English;x0=enS_v101.xml;d1=Spanish;x1=esS_v101.xml /
Dictionary_Server_Script
```

8

Configuring Dial Plans

Dial plans determine how the digits are interpreted and transmitted. They also determine whether the dialed number is accepted or rejected. You can use a dial plan to facilitate dialing or to block certain types of calls such as long distance or international.

If the Cisco SPA 500 Series and WIP310 IP Phones are part of the Cisco SPA 9000 Voice System, dial plans are configured on the Cisco SPA 9000. In installations where a Cisco SPA 9000 is not present (such as IP Centrex installations), installations where the phones are removed from the SPA 9000 (such as by a VPN), or other situations, dial plans can be configured on the IP phone using the web administration user interface.

For more information on using dial plans on the Cisco SPA 9000 Voice System, see the *Cisco SPA 9000 Voice System Administration Guide*. See the **Appendix C, "Where to Go From Here,"** for the location of the document.

This section includes information that you need to understand dial plans, as well as procedures for configuring your own dial plans. This section includes the following topics:

About Dial Plans

This section provides information to help you understand how dial plans are implemented.

The Cisco SPA 500 Series and WIP310 IP Phones and the SPA 9000 are involved in applying various levels of the dial plans and process the digits sequence in the same manner.

When a user lifts a handset or presses a speaker button on the IP phone, the following sequence of events begins:

1. The phone begins collecting the dialed digits. The inter-digit timers starts tracking the time that elapses between digits.
2. If the inter-digit timer value is reached, or if another terminating event occurs, the phone compares the dialed digits with the IP phone's dial plan. (This dial plan is configured in the web administration user interface in the **Voice** tab, on the tab for each extension (**Ext N**), under the **Dial Plan** section.)

   If the phone is part of a Cisco SPA 9000 system:
3. If the phone dial plan allows the call to process, the dialed numbers are sent to the Cisco SPA 9000.
4. The Cisco SPA 9000 compares the dialed digits to the CALL ROUTING RULE (on the *SPA 9000 Voice > SIP* page, *PBX Parameters* section).
5. If the call routing rule allows the call to process, then the Cisco SPA 9000 compares the dialed digits to the LINE INTERFACE dial plan (on the *Cisco SPA 9000 Voice > Line N* page, *Dial Plan* section).
6. The Cisco SPA 9000 uses the information in the line dial plan to manipulate the number (for example, to remove steering digits) and then transmits the number.

Refer to the following topics:

- **"Digit Sequences," on page 170**
- **"Digit Sequence Examples," on page 172**
- **"Acceptance and Transmission of the Dialed Digits," on page 174**
- **"Dial Plan Timer (Off-Hook Timer)," on page 175**
- **"Interdigit Long Timer (Incomplete Entry Timer)," on page 176**
- **"Interdigit Short Timer (Complete Entry Timer)," on page 177**

Digit Sequences

A dial plan contains a series of digit sequences, separated by the | character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan consists of a series of elements, which are individually matched to the keys that the user presses.

NOTE White space is ignored, but may be used for readability.

Digit Sequence	Function
`0 1 2 3 4 5 6 7 8 9 0 * #`	Enter any of these characters to represent a key that the user must press on the phone keypad.
`x`	Enter `x` to represent any character on the phone keypad.
`[sequence]`	Enter characters within square brackets to create a list of accepted key presses. The user can press any one of the keys in the list. ▪ Numeric range For example, you would enter `[2-9]` to allow the user to press any one digit from 2 through 9. ▪ Numeric range with other characters For example, you would enter `[35-8*]` to allow the user to press 3, 5, 6, 7, 8, or *.
`.` (period)	Enter a period for element repetition. The dial plan accepts 0 or more entries of the digit. For example, `01.` allows users to enter 0, 01, 011, 0111, and so on.

Digit Sequence	Function
<dialed:substituted>	For sequence substitution, use this format to indicate that certain dialed digits are replaced by other characters when the sequence is transmitted. The dialed digits can be zero or more characters. **EXAMPLE 1:** <8:1650>xxxxxxx When the user presses 8 followed by a seven-digit number, the system automatically replaces the dialed 8 with 1650. If the user dials **85550112**, the system transmits **16505550112**. **EXAMPLE 2:** <:1>xxxxxxxxxx In this example, no digits are replaced. When the user enters a 10-digit string of numbers, the number 1 is added at the beginning of the sequence. If the user dials **9725550112**, the system transmits **19725550112**
, (comma)	For an intersequence tone, enter a comma between digits to play an "outside line" dial tone after a user-entered sequence. **EXAMPLE:** 9, 1xxxxxxxxx An "outside line" dial tone is sounded after the user presses 9, and the tone continues until the user presses 1.
! (exclamation point)	For number barring, enter an exclamation point to prohibit a dial sequence pattern. **EXAMPLE:** 1900xxxxxx! The system rejects any 11-digit sequence that begins with 1900.
*xx	Enter an asterisk to allow the user to enter a 2-digit star code.
S0 or L0	For Interdigit Timer Master Override, enter S0 to reduce the short inter-digit timer to 0 seconds, or enter L0 to reduce the long inter-digit timer to 0 seconds.
P	For a pause, enter P followed by a number and a space. The duration of the pause is the specified number of seconds. This feature is typically used for implementation of a hot line and warm line, with 0 delay for the hot line and a non-zero delay for a warm line. **EXAMPLE:** P5

NOTE The Cisco SPA 9000 and the Cisco IP phones implicitly append the vertical code sequences entered in the regional parameter settings to the end of the dial plan. Likewise, if Enable_IP_Dialing is enabled, then IP dialing is also accepted on the associated line.

Digit Sequence Examples

The following examples show digit sequences that you can enter in a dial plan.

In a complete dial plan entry, sequences are separated by a pipe character (|), and the entire set of sequences is enclosed within parentheses.

EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

- Extensions on your system

  EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

  `[1-8]xx` Allows a user dial any three-digit number that starts with the digits 1 through 8. If your system uses four-digit extensions, you would instead enter the following string: **[1-8]xxx**

- Local dialing with seven-digit number

  EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]111)`

  `9, xxxxxxx` After a user presses 9, an external dial tone sounds. The user can enter any seven-digit number, as in a local call.

- Local dialing with 3-digit area code and a 7-digit local number

  EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

9, <:1>[2-9]xxxxxxxxx This example is useful where a local area code is required. After a user presses 9, an external dial tone sounds. The user must enter a 10-digit number that begins with a digit 2 through 9. The system automatically inserts the 1 prefix before transmitting the number to the carrier.

- Local dialing with an automatically inserted 3-digit area code

  EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

  8, <:1212>xxxxxxx This is example is useful where a local area code is required by the carrier but the majority of calls go to one area code. After the user presses 8, an external dial tone sounds. The user can enter any seven-digit number. The system automatically inserts the 1 prefix and the 212 area code before transmitting the number to the carrier.

- U.S. long distance dialing

  EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

  9, 1 [2-9] xxxxxxxxx After the user presses 9, an external dial tone sounds. The user can enter any 11-digit number that starts with 1 and is followed by a digit 2 through 9.

- Blocked number

  EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

  9, 1 900 xxxxxxx ! This digit sequence is useful if you want to prevent users from dialing numbers that are associated with high tolls or inappropriate content, such as 1-900 numbers in the U.S.. After the user press 9, an external dial tone sounds. If the user enters an 11-digit number that starts with the digits 1900, the call is rejected.

- U.S. international dialing

  EXAMPLE: `( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )`

  9, 011xxxxxx. After the user presses 9, an external dial tone sounds. The user can enter any number that starts with 011, as in an international call from the U.S.

- Informational numbers

  EXAMPLE: ([1-8]xx | 9, xxxxxxx **|** 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | **0 | [49]11**)

  0 | [49]11 This example includes two digit sequences, separated by the pipe character. The first sequence allows a user to dial 0 for an operator. The second sequence allows the user to enter 411 for local information or 911 for emergency services.

Acceptance and Transmission of the Dialed Digits

When a user dials a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. As more digits are entered by the user, the set of candidates diminishes until only one or none are valid. When a terminating event occurs, the IP PBX either accepts the user-dialed sequence and initiates a call, or else rejects the sequence as invalid. The user hears the reorder (fast busy) tone if the dialed sequence is invalid.

The following table explains how terminating events are processed.

Terminating Event	Processing
The dialed digits do not match any sequence in the dial plan.	The number is rejected.
The dialed digits exactly match one sequence in the dial plan.	▪ If the sequence is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. ▪ If the sequence is blocked by the dial plan, the number is rejected.
A timeout occurs.	The number is rejected if the dialed digits are not matched to a digit sequence in the dial plan within the time specified by the applicable interdigit timer. ▪ The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan. The default value is 10 seconds. ▪ The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. The default value is 3 seconds.

Terminating Event	Processing
The user presses the # key or the **dial** softkey on the phone display.	▪ If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan. ▪ If the sequence is incomplete or is blocked by the dial plan, the number is rejected.

Dial Plan Timer (Off-Hook Timer)

You can think of the Dial Plan Timer as "the off-hook timer." This timer starts counting when the phone goes off hook. If no digits are dialed within the specified number of seconds, the timer expires and the null entry is evaluated. Unless you have a special dial plan string to allow a null entry, the call is rejected. The default value is 5.

Syntax for the Dial Plan Timer

SYNTAX: `(Ps<:n> | dial plan )`

- **s:** The number of seconds; if no number is entered after P, the default timer of 5 seconds applies.
- **n:** (optional): The number to transmit automatically when the timer expires; you can enter an extension number or a DID number. No wildcard characters are allowed because the number will be transmitted as shown. If you omit the number substitution, <:n>, then the user hears a reorder (fast busy) tone after the specified number of seconds.

Examples for the Dial Plan Timer

- Allow more time for users to start dialing after taking a phone off hook.

  EXAMPLE: `(P9 | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  P9 After taking a phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the user hears a reorder (fast busy) tone. By setting a longer timer, you allow more time for users to enter the digits.

- Create a hotline for all sequences on the System Dial Plan

  EXAMPLE: `(P9<:23> | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

P9<:23> After taking the phone off hook, a user has 9 seconds to begin dialing. If no digits are pressed within 9 seconds, the call is transmitted automatically to extension 23.

- Create a hotline on a line button for an extension

  EXAMPLE: (P0 <:1000>)

  With the timer set to 0 seconds, the call is transmitted automatically to the specified extension when the phone goes off hook. Enter this sequence in the Phone Dial Plan for Ext 2 or higher on a client station.

Interdigit Long Timer (Incomplete Entry Timer)

You can think of this timer as the "incomplete entry" timer. This timer measures the interval between dialed digits. It applies as long as the dialed digits do not match any digit sequences in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated as incomplete, and the call is rejected. The default value is 10 seconds.


NOTE This section explains how to edit a timer as part of a dial plan. Alternatively, you can modify the Control Timer that controls the default interdigit timers for all calls. See **"Resetting the Control Timers," on page 179**.

Syntax for the Interdigit Long Timer

SYNTAX: L:*s*, (*dial plan*)

- **s:** The number of seconds; if no number is entered after L:, the default timer of 5 seconds applies.
- Note that the timer sequence appears to the left of the initial parenthesis for the dial plan.

Example for the Interdigit Long Timer

EXAMPLE: L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)

L:15, This dial plan allows the user to pause for up to 15 seconds between digits before the Interdigit Long Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

Interdigit Short Timer (Complete Entry Timer)

You can think of this timer as the “complete entry” timer. This timer measures the interval between dialed digits. It applies when the dialed digits match at least one digit sequence in the dial plan. Unless the user enters another digit within the specified number of seconds, the entry is evaluated. If it is valid, the call proceeds. If it is invalid, the call is rejected. The default value is 3 seconds.

Syntax for the Interdigit Short Timer

- **SYNTAX 1:** S:*s,* `( dial plan )`

  Use this syntax to apply the new setting to the entire dial plan within the parentheses.

- **SYNTAX 2:** *sequence* `Ss`

  Use this syntax to apply the new setting to a particular dialing sequence.

  s: The number of seconds; if no number is entered after S, the default timer of 5 seconds applies.

Examples for the Interdigit Short Timer

- Set the timer for the entire dial plan.

  EXAMPLE: `S:6, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `S:6,` While entering a number with the phone off hook, a user can pause for up to 15 seconds between digits before the Interdigit Short Timer expires. This setting is especially helpful to users such as sales people, who are reading the numbers from business cards and other printed materials while dialing.

- Set an instant timer for a particular sequence within the dial plan.

  EXAMPLE: `(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxS0 | 9,8,011xx. | 9,8,xx.|[1-8]xx)`

  `9,8,1[2-9]xxxxxxxxxS0` With the timer set to 0, the call is transmitted automatically when the user dials the final digit in the sequence.

Editing Dial Plans on the IP Phone

You can edit dial plans and can modify the control timers. To edit the dial plans on the IP phone:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click the **Ext *N*** tab, where *N* is the extension being configured.

STEP 4 In the Dial Plan section, enter the digit sequences in the *Dial Plan* field. For more information and examples, see **"Digit Sequences," on page 170**.

The default (US-based) system-wide dial plan appears automatically in the field. You can delete digit sequences, add digit sequences, or replace the entire dial plan with a new dial plan. For more information and examples, see **"Digit Sequences," on page 170**.

Separate each digit sequence with a pipe character, and enclose the entire set of digit sequences within parentheses. Refer to the following example:

```
(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxx | 9,8,011xx.
| 9,8,xx.|[1-8]xx)
```

STEP 5 (Optional) Enter the Caller ID Map—Inbound caller ID numbers can be mapped to a different string. For example, a number that begins with +44xxxxxx can be mapped to 0xxxxxx. This feature has the same syntax as the Dial Plan parameter. With this parameter, you can specify how to map a caller ID number for display on screen and recorded into call logs. (Not applicable to WIP310.)

STEP 6 (Optional) Enable IP dialing—Enable or disable IP dialing. Defaults to no.

STEP 7 (Optional) Emergency Number—Enter a comma-separated list of emergency numbers. When one of these numbers is dialed, the unit disables processing of *CONF*, *HOLD*, and other similar softkeys or buttons to avoid accidentally putting the current call on hold. The phone also disables hook flash event handling. Only the far end can terminate an emergency call. The phone is restored to normal after the call is terminated and the phone is back on-hook.

Maximum number length is 63 characters. Defaults to blank (no emergency number). (Not applicable to WIP310.)

STEP 8 Click **Submit All Changes**. The phone reboots.

STEP 9 If you need to configure a dial plan for any other extensions on the phone (depending on the model), click the appropriate *Extension* tab, enter the dial plan, and submit the changes.

STEP 10 Verify that you can successfully complete a call using each digit sequence that you entered in the dial plan.

NOTE If you hear a reorder (fast busy) tone, you need to review your entries and modify the dial plan appropriately. See **"Digit Sequences," on page 170**.

Resetting the Control Timers

You can use the following procedure to reset the default timer settings for all calls.

NOTE If you need to edit a timer setting only for a particular digit sequence or type of call, you can edit the dial plan. See **"About Dial Plans," on page 168**.

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login** and **advanced**.

STEP 3 Click **Voice tab > Regional**.

STEP 4 Scroll down to the *Control Timer Values* section.

STEP 5 Enter the desired values in the *Interdigit Long Timer* field and the *Interdigit Short Timer* field. Refer to the definitions at the beginning of this section.

9

Configuring the Cisco SPA 500S Attendant Console

The Cisco SPA 500S is a 32-button attendant console for the Cisco SPA 500 Series IP Phones. The Cisco SPA 500S works in both SIP and SPCP mode. The Cisco SPA 500S connects to the phone with the attachment arm provided (not shown). It obtains power directly from the phone and does not require a separate power supply. Two Cisco SPA 500S units can be attached to a single phone to monitor a total of 64 separate lines.

For more information about installing and configuring the Cisco SPA 500S with a Cisco SPA 9000 system, see the *Cisco SPA 9000 Voice System Installation and Configuration Guide*.

This chapter contains the following sections:

Cisco SPA 500S Features

Cisco SPA 500S features include:

- 32 programmable speed-dial or direct station select (DSS) buttons/LEDs
- Three-color LEDs (red, green, and orange)
- Support for BroadSoft Busy Lamp Field (BLF)
- Support for Line Monitoring
- Illuminated line status monitoring (Idle, Ringing, Busy, Null, or Registration Error)
- One-touch Call Transfer—Incoming calls can be immediately transferred to the target destination by pressing a button/key as assigned on the Cisco SPA 500S.

The following table describes Cisco SPA 500S ports and LEDs.

.

Port/LED	Meaning
AUX IN	Connects to the phone.
AUX OUT	Connects to a second Cisco SPA 500S unit (optional)
Solid Green	Idle
Solid Red	In-use
Blinking Red	Ringing
Orange	Solid: not registered. Blinking: configuration error.
Off	Not configured

Setting Up the Cisco SPA 500S Attendant Console

To configure the server to use the Cisco SPA 500S, configure each extension that will be monitored by the attendant console. The Cisco SPA 500S is a SIP subscriber in relation to each SIP proxy server, which allows the Cisco SPA 500S to receive NOTIFY messages from the SIP proxy that indicate the status of each monitored phone. In general, the SIP proxy is identified by its IP address, or through a hostname if DNS is configured. The way in which each phone and extension is identified is vendor-specific.

To set up the Cisco SPA 500S attendant console:

STEP 1 Complete the physical installation of the Cisco SPA 500S unit, which connects it to the phone. For instructions on installing the Cisco SPA 500S and an introduction to its use, refer to the *Cisco SPA 500S Quick Start Guide* or the phone user guides available on Cisco.com. See **Appendix C, "Where to Go From Here,"** for a list of those guides.

STEP 2 Configure one of the following SIP proxy servers:

- Cisco SPA 9000—See **Configuring the Cisco SPA 9000 for the Cisco SPA 500S, page 183** (verify that your version of the Cisco SPA 9000 supports the Cisco SPA 500S).
- BroadSoft—See **Configuring the BroadSoft Server for the Cisco SPA 500S, page 183**.
- Asterisk—See **Configuring the Asterisk Server for the Cisco SPA 500S, page 184**.

STEP 3 Configure the Cisco SPA 500S using the web UI. The web server must be connected to the phone to which the Cisco SPA 500S is physically attached.

NOTE CTI must be enabled on the phone for an attached Cisco SPA 500S to properly monitor the IP phone's line status when the SIP proxy server type is set to Cisco SPA 9000. See the "Configuring SIP" section on page 89.

Configuring the Cisco SPA 9000 for the Cisco SPA 500S

You must still enable Computer Telephony Integration (CTI) on the Cisco SPA 9000 web UI, as shown in the following procedure:

STEP 1 Connect to the web UI for the Cisco SPA 9000.

STEP 2 Click **Admin Login** on the web UI page.

STEP 3 If necessary, enter **admin** and your password, then **Advanced**.

STEP 4 Click the **SIP** tab.

STEP 5 In the *SIP Parameters* section, select **yes** from the *CTI Enable* drop-down list.

STEP 6 Click **Submit All Changes**.

Configuring the BroadSoft Server for the Cisco SPA 500S

The BroadSoft server requires you to assign IP phone users to the Busy Lamp (BLF) Monitor Users List. The BroadSoft server sends updates on the status of each phone on this list to the Cisco SPA 500S, which subscribes for this service.

To configure the BroadSoft server to support the Cisco SPA 500S:

STEP 1 On the BroadSoft server, in the user profile used by the phone to register with the BroadSoft server, select **Assign Services**.

STEP 2 On the Assign Services page, from the Available Services column, move **Busy Lamp** to the User Services column.

STEP 3 Define the List URI used by the Cisco SPA 500S to register for BLF monitoring service with the BroadSoft server. This value must match the value entered following the sub = keyword (for example, cisco_list). Select the domain from the drop-down list to match the Unit Key.

NOTE If you configure more than one monitored list on the BroadSoft server, use the vid= keyword in each unit/keyconfiguration script to specify the phone extension to use for each list.

STEP 4 On the Busy Lamp Field page, move users that need to be monitored from the Available Users column to the Monitored Users column.

STEP 5 Click the **Add** (or **Add All**) button to move each user to the Monitored Users column. The Directory Number (DN) associated with each user account when it is created on the BroadSoft Server is shown in parenthesis in the Monitored Users list. You use this DN to identify the specific phone assigned to each key on the Cisco SPA 500S.

STEP 6 Save and enable your configuration changes on the BroadSoft server.

See also the **"Configuring BroadSoft Busy Lamp Field Auto-Configuration" section on page 189**.

Configuring the Asterisk Server for the Cisco SPA 500S

To configure the Asterisk server to allow the Cisco SPA 500S to register for BLF monitoring:

STEP 1 Add a context in the extensions.conf file.

STEP 2 Add a `Subscribecontext` command to point to the context in the sip.conf file.

STEP 3 Configure the Cisco SPA 500S to register with the Asterisk server (see **"Configuring the Cisco SPA 500S" section on page 185**.

The following example context uses "home" for extension 3500. This is entered in the file extensions.conf:

```
[home]
exten => 3500,1,Dial(SIP/3500)
exten => 3500,hint,SIP/3500
exten => 3500,2,Voicemail,u3500
exten =>3500,1,3,hangup
...
```

In the following example, extension 3500 is used to add `Subscribecontext` to point to the context.

This is entered in the file sip.conf:

```
[3500]
type=friend
secret=3500
callerid="spa3500"<3500>
nat=no
context=home
mailbox=3500
Subscribecontext=home
...
...
```

Configuring the Cisco SPA 500S

Complete the configuration required for the extensions on your IP PBX and obtain the following information:

- IP PBX IP address or other hostname
- Phone extension numbers

To configure the Cisco SPA 500S:

NOTE Steps 1 through 4 are only required when the *Server Type* field is set to **SPA9000**. These steps are not required for other server types such as BroadSoft and Asterisk.

STEP 1 Connect to the web UI for the phone to which the Cisco SPA 500S is connected.

STEP 2 Click **Admin/Advanced** on the web UI page.

STEP 3 Click the **SIP** tab.

STEP 4 Select **yes** from the *CTI Enable* drop-down list.

STEP 5 Click the **Attendant Console** tab.

STEP 6 Select **yes** from the *Unit 1 Enable* drop-down list. If you have installed two Cisco SPA 500S units, also select **yes** from the *Unit 2 Enable* drop-down list.

STEP 7 Select your *Server Type* from the drop-down list:

- SPA9000
- BroadSoft
- Asterisk

STEP 8 Make sure that **no** is selected for *Test Mode Enable*. This option is disabled by default. You cannot complete the software configuration for the Cisco SPA 500S if this option is enabled. (You can use Test Mode Enable later to test the Cisco SPA 500S.)

STEP 9 Create a configuration script for each target extension or user you want to monitor using the Cisco SPA 500S. Enter this script in the appropriate field for each unit/key. See **"Unit/Key Configuration Scripts" section on page 186**.

STEP 10 Click **Submit All Changes**.

Unit/Key Configuration Scripts

By default, all LEDs on the Cisco SPA 500S are assigned to the first configured extension on the phone to which it is connected. Assign the LEDs to any of the other five extensions on the phone that you want to monitor using the Cisco SPA 500S.

The configuration script is composed of the following keywords, followed by an equal sign (=) and separated by semicolons (;):

- fnc—defines which of the following functions are enabled for the specified key [separate more than one function with a plus sign (+)]:
  - blf—busy lamp field function used for monitoring line activity
  - sd—speed dial function
  - cp—call pickup (if supported by the SIP proxy server). Call pickup (cp) must be supported by the SIP proxy server and be used with blf in the configuration. The syntax is fnc=blf+cp.
- sub—Use this keyword to identify the phones to be monitored). Its value and syntax is stationName@$PROXY, where system variable $PROXY contains the proxy server IP and port (e.g. 192.168.8.101:6060).

NOTE Unit/key LEDs will not light without the “sub” keyword. (Not required for speed dials.)

- usr or ext (optional)—Use one of these keywords to identify the specific users or extensions to be monitored. Its value and syntax is extensionNumber@$PROXY, where system variable $PROXY contains the proxy server IP and port (e.g. 192.168.8.101:6060). (The *usr* and *ext* keywords are interchangeable.) If the ext parameter is not used, all extensions on the phone are monitored.
- nme (optional)— Use this field with the Cisco SPA 9000 to identify any alias that has been assigned to the extension in the IP phone configuration.The nme parameter indicates the extension name, which in this case is the same as the station name.
- vid (optional)— All LEDs on the Cisco SPA 500S use phone extensions that they are assigned to. By default, LEDs on the Cisco SPA 500S are assigned to the first configured extension on the connected phone. You can optionally assign LEDs to any other phone extensions using vid=keyword. Use this field to identify the phone extension to use with the monitored list specified by the sub= keyword, when more than one BLF monitored list is configured on the SIP proxy server. The possible values are 1 to 6, corresponding to each of the six extensions available on the phone. Only use the vid= keyword in the first entry assigned to each phone extension. Subsequent keys will use the same extension. See **“Attendant Console Parameters” section on page 190**.

Assigning Cisco SPA 500S LEDs to Phone Extensions

By default, all 32 keys on the Cisco SPA 500S are assigned to the first extension on the IP phone (extension 101 based on the default multicast autoconfiguration).

To limit the number of LEDs assigned to the first extension, use the vid=1 keyword. Then use the vid=2 keyword to assign the next set of keys to the second extension. The numeric values correspond to the default extensions on the phone as follows:

- vid=1—extension 101
- vid=2—extension 102
- vid=3—extension 103
- vid=4—extension 104
- vid=5—extension 105
- vid=6—extension 106

Cisco SPA 9000 Syntax

Find more complete information in the *Cisco SPA 9000 Voice System Installation and Configuration Guide*.

The following entry enables speed dialing, BLF monitoring, and call pick up on a Cisco SPA 9000 server with:

- IP address 192.168.1.101
- station name phone1
- extension 101
- Cisco SPA 500S unit/key using the phone's extension 2

Example:

```
fnc=sd+blf+cp;sub=phone1@$PROXY;usr=101@$PROXY;nme=phone1;vid=2
```

BroadSoft syntax

For example, the following enables speed dialing and BLF monitoring, with a BLF monitoring list URI of marketing, for the user account reception, on a BroadSoft server with the IP address 192.168.100.1:

```
fnc=sd+blf;sub=marketing@192.168.100.1;usr=reception@192.168.100.1
```

The ***nme*** keyword is not used because the BroadSoft server uses the user account name assigned to the BLF monitoring list.

Note that you can configure a list of BLF subscriptions automatically using a URI (rather than individually configuring each BLF entry). See the **"Configuring BroadSoft Busy Lamp Field Auto-Configuration" section on page 189**.

Asterisk syntax

The following is an example entry for a Asterisk server. This entry enables speed dialing, BLF monitoring, and call pickup on a Asterisk server with the IP address 192.168.1.11:

```
fnc=sd+blf+cp;sub=35890@192.168.1.11;nme=35890
```

Configuring BroadSoft Busy Lamp Field Auto-Configuration

Rather than configuring each BLF key individually, you can enter a single SUBSCRIBE URI and automatically generate configuration scripts for BLF keys for all users on the monitored list.

To configure BLF auto-configuration:

STEP 1 Log in to the web administration interface.

STEP 2 Click **Admin Login**.

STEP 3 Click **advanced**.

STEP 4 Click the **Att Console** tab.

STEP 5 In the BLF List URI field, enter the URI to generate BLF keys:

```
listname@domain.com;vid=2
```

Where:

- listname: Name of the list.
- domain.com: Name of the domain.
- vid: Assigns keys to the extension. By default, the SUBSCRIBE is sent when "Ext 1" is registered. You must set the "vid=" to a different value to change this behavior.

For example:

```
mylist@broadsoft.com;vid=2
```

STEP 6 Click **Submit All Changes**.

Attendant Console Parameters

Parameters in the Attendant Console web page are described in the following table. For information about Unit/Key syntax, see the previous sections.

.

Parameter	Description
Subscribe Expires	Specifies how long the subscription remains valid. After the specified period of time, elapses, the Cisco SPA 500S initiates a new subscription. Defaults to 1800.
Subscribe Retry Interval	Specifies the length of time to wait to try again if subscription fails.
Unit 1 Enable	Enables or disables the first Cisco SPA 500S unit (each phone can have up to two Cisco SPA 500S units attached).
Unit 2 Enable	Enables or disables the second Cisco SPA 500S unit (each phone can have up to two Cisco SPA 500S units attached).
Subscribe Delay	Length of delay before attempting to subscribe. Defaults to 1.

Parameter	Description
Server Type	Selects the type of server used (SPA9000, BroadSoft, or Asterisk).
Test Mode Enable	Enables or disables test mode. When test mode is enabled, the LEDs are turned on when keys are pressed, going from off to green to red, and back to off. In test mode, when all the buttons on the attendant console are returned to off, all the keys become orange. The phone must be rebooted after the test is completed.
Attendant Console Call Pickup Code	The star code used for picking up a ringing call. Defaults to *98.
BLF List URI	Automatically configures BLF subscriptions for all users on a monitored list.
Unit 1 Key 1-32	Enter a strings that define the extension and other parameters associated with each lighted button on the first Cisco SPA 500S unit. Keywords and values are case-sensitive. The configuration script is described in **"Unit/Key Configuration Scripts" section on page 186**.

Monitoring the Cisco SPA 500S

To display the status of the Cisco SPA 500S, click the Attendant Console Status link on the GUI. The status of each attendant console attached (Unit 1 and Unit 2) is shown. Parameters are read-only.

Cisco SPA 500S Unit Monitoring Notes

The following table describes each parameter; both units display the same parameters.

Parameter	Description
Unit Enable	Displays if the Unit is enabled or disabled.
Subscribe Expires	Displays when the current subscription expires. After the subscription expires, the Cisco SPA 500S automatically requests a new subscription.
HW Version	Displays the version of the hardware.
Unit Online	Displays whether the unit is connected or not.
Subscribe Retry Interval	Displays the length of time the Cisco SPA 500S waits to try again if subscription fails.
SW Version	Displays the version of the software currently running on the unit.
Key Name	Displays the name assigned to each key (1-32) on the Cisco SPA 500S attendant console unit.
Type	Displays the function enabled for each key (1-32) on the Cisco SPA 500S attendant console unit.
Line	Displays the extension assigned to each key (1-32) on the Cisco SPA 500S attendant console unit.
Station	Displays the subscribe URI configured for each key (1-32) on the Cisco SPA 500S attendant console unit.
Subscribe	Displays the subscription status of the unit/key. The value can be Yes, Fail, or No. No indicates that the feature/function (fnc) of that line does not require a subscription (such as speed dial).

A

Creating an LED Script

LED Script

The LED script describes the color and blinking pattern of a Line Key LED. Each script contains a number of fields separated by a semicolon(;). White spaces are ignored. Each field has the syntax *<field-name> = <field-value>*. The allowed *field-name* and corresponding *field-values* are listed below:

c=o|r|g|a

This field sets the **color** of the LED. The 4 choices are:

- o = off
- r = red
- g = green
- a = amber (orange)

p=n[b]|s[b]|f[b]|d[b]|u[d]

This field sets the blinking **pattern** of the LED. The 4 choices are:

- nb = no blink (steady on or off)
- sb = slow blink (1s on and 1s off)
- fb = fast blink (100ms on and 100ms off)
- ud = user-defined (according to the contents of the u field)

u=on/off/on/off/etc.

This is a user-defined blinking pattern used only when p = ud. It consists of up to 4 pairs of on/off duration in seconds with up to 2 decimal places; each value is separated by a forward slash (/).

LED Script Examples

Example 1

```
c=r;p=sb
```

Color is red and pattern is slow blink.

Example 2

```
c=o
```

LED is off.

Example 3

```
c=g
```

Color is green and pattern is steady on (default).

Example 4

```
c=a;p=ud;u=.1/.1/.1/.1/.1/.9
```

Color is amber (orange) and the blink pattern is: 100ms on, 100ms off, 100ms on, 100ms off, 100ms on, 900ms off

LED Pattern

The administrator can also specify a different color and pattern for each of the following states of the call appearance.

- Idle: This call appearance is not in use. It can be used to make outbound call on this station
- Local Seized: This call appearance has been seized by this station to prepare for an outbound call
- Local Progressing: This station is making an outbound call that is progressing
- Local Active: This station is engaged in a connected call on this call appearance
- Local Ringing: This station is ringing for an incoming call on this call appearance
- Local Held: This station has placed this call appearance on hold

- Remote Seized: This call appearance has been seized by another station to prepare for an outbound call
- Remote Progressing: Another station is making a call on this call appearance and is progressing
- Remote Active: Another station is engaged in a connected call on this call appearance
- Remote Ringing: Another station is ringing for an incoming call to this call appearance
- Remote Held: Another station has placed this call appearance on hold
- Remote Undefined: The share call state is not known (this station is waiting for a notification from the application server)
- Registration Failed: This station has failed to register with the proxy server for the corresponding extension
- Registering: The station is attempting registration with the proxy server for the corresponding extension.
- Disabled: This line key on this station is disabled
- Call Back: A call back (repeat dialing) operation is currently active on this call appearance

B

Cisco SPA 500 Series and Wireless IP Phone Field Reference

This appendix describes the fields within each section of the following web UI pages:

Voice Tab

NOTE For information about the Provisioning page, see the *Cisco Small Business IP Telephony Devices Provisioning Guide*.

Info Tab

This section describes the fields for the following headings on the Info tab:

NOTE The fields on this tab are read-only and cannot be edited.

System Information

Parameter	Description
DHCP	Indicates if DHCP is enabled. **NOTE** Not applicable to Cisco SPA 525G or WIP310.
Connection Type (WIP310/ Cisco SPA 525G only)	Indicates the type of internet connection for the phone: ▪ DHCP ▪ Static IP ▪ PPPoE (not applicable to WIP310)
Current IP	Displays the current IP address assigned to the IP phone.
Host Name	Displays the current host name assigned to the IP phone (defaults to SipuraSPA).
Domain	Displays the network domain name of the IP phone.
Current Netmask	Displays the network mask assigned to the IP phone.

Parameter	Description
Current Gateway	Displays the default router assigned to the IP phone.
Primary DNS	Displays the primary DNS server assigned to the IP phone.
Secondary DNS	Displays the secondary DNS server assigned to the IP phone.
NTP Enable (Cisco SPA 525G only)	Shows if Network Time Protocol is enabled.
Primary NTP Server (Cisco SPA 525G only)	IP Address of the primary NTP server.
Secondary NTP Server (Cisco SPA 525G only)	IP Address of the secondary NTP server.
TFTP Server (Cisco SPA 525G only)	Address of the TFTP server for provisioning.
Bluetooth Enabled (Cisco SPA 525G only)	Shows if Bluetooth is enabled.
Bluetooth Firmware Version (Cisco SPA 525G only)	Displays the Bluetooth firmware version.
Bluetooth Connected (Cisco SPA 525G only)	Shows if a Bluetooth device is connected to the phone.
Bluetooth MAC (Cisco SPA 525G only)	Shows the hardware address of the Bluetooth device.
Connected Device ID (Cisco SPA 525G only)	Shows the name of the connected Bluetooth device.
Wireless Enabled (Cisco SPA 525G only)	Shows if Wireless-G is enabled on the phone.
Wireless Connected (Cisco SPA 525G only)	Shows if the phone is connected to the wireless network.
Wireless MAC (Cisco SPA 525G only)	Shows the hardware address of the Wireless-G controller.
SSID (Cisco SPA 525G only)	Shows the SSID, or name of the wireless router to which the phone is connected.

Parameter	Description
Standard Channel (Cisco SPA 525G only)	Shows the wireless channel being used in the wireless connection.
Security Mode (Cisco SPA 525G only)	Shows if wireless security is configured on the phone (yes or no).

Network Configuration (SPCP)

Parameter	Description
TFTP Server	Address of the TFTP server for provisioning.
Call Manager	IP address of the Unified Communications server.
Directories URL	Populated by the Unified Communications Server; points to the directory application server.
Services URL	Populated by the Unified Communications Server; points to the Cisco XML application server.
Authentication URL	Populated by the Unified Communications Server; points to the authentication server.
DHCP Address Released	Populated by the Unified Communications Server; indicates if the DHCP address has been released.

VPN Status

Parameter	Description
VPN Connected	Indicates if the phone is connected to a VPN.
Client Address	IP address given to the phone from the VPN server.
Client Netmask	Netmask given to the phone from the VPN server.
Bytes Sent	Size of data sent from the phone.
Bytes Recv	Size of data received by the phone.

Product Information

Parameter	Description
Product Name	Model number of the IP phone.
Serial Number	Serial number of the IP phone.
Software Version	Version number of the IP phone software.
Hardware Version	Version number of the IP phone hardware.
MAC Address	Hardware address of the IP phone.
Client Certificate	Status of the client certificate, which authenticates the IP phone for use in the ITSP network. This field indicates if the client certificate is properly installed in the IP phone.
Customization	For an RC unit, this field indicates whether the unit has been customized or not. Pending indicates a new RC unit that is ready for provisioning. If the unit has already retrieved its customized profile, this field displays the name of the company that provisioned the unit.
Licenses	Indicates any additional licenses that you have installed in the IP phone.

Phone Status

Parameter	Description
Current Time	Current date and time of the system; for example, 10/3/2003 16:43:00.
Elapsed Time	Total time elapsed since the last reboot of the system; for example, 25 days and 18:12:36.
Broadcast Pkts Sent	Total number of broadcast packets sent.
Broadcast Bytes Sent	Total number of broadcast packets received.
Broadcast Pkts Recv	Total number of broadcast bytes sent.

Parameter	Description
Broadcast Bytes Recv	Total number of broadcast bytes received and processed.
Broadcast Pkts Dropped	Total number of broadcast packets received but not processed. Most codecs can handle up to 5% random packet drops as long as the packets are random and not in groups of two or more. Concurrent packet drops result in voice quality issues.
Broadcast Bytes Dropped	Total number of broadcast bytes received but not processed.
RTP Packets Sent	Total number of RTP packets sent (including redundant packets).
RTP Bytes Sent	Total number of RTP packets received (including redundant packets).
RTP Packets Recv	Total number of RTP bytes sent.
RTP Bytes Recv	Total number of RTP bytes received.
SIP Messages Sent	Total number of SIP messages sent (including retransmissions).
SIP Bytes Sent	Total number of SIP messages received (including retransmissions).
SIP Messages Recv	Total number of bytes of SIP messages sent (including retransmissions).
SIP Bytes Recv	Total number of bytes of SIP messages received (including retransmissions).
External IP	External IP address used for NAT mapping.
Operational VLAN ID	ID of the VLAN currently in use if applicable. **NOTE** Not applicable to WIP310.

Ext Status

The following parameters show for each extension on the phone.

Parameter	Description
Registration State	Shows “Registered” if the phone is registered, “Not Registered” if the phone is not registered to the ITSP.
Last Registration At	Last date and time the line was registered.
Next Registration In	Number of seconds before the next registration renewal.
Message Waiting	Indicates whether the phone user has a new voice mail waiting: Yes or No. This is updated when voice mail notification is received.
Mapped SIP Port	Port number of the SIP port mapped by NAT.

Line/Call Status

The following parameters show for each line and call on the phone.

Parameter	Description
Call State	Status of the call.
Tone	Type of tone used by the call.
Encoder	Codec used for encoding.
Decoder	Codec used for decoding.
Type	Direction of the call.
Remote Hold	Indicates whether the far end has placed the call on hold.
Callback	Indicates whether the call was triggered by a call back request.
Peer Name	Name of the internal phone.

Parameter	Description
Peer Phone	Phone number of the internal phone.
Duration	Duration of the call.
Packets Sent	Number of packets sent.
Packets Recv	Number of packets received.
Bytes Sent	Number of bytes sent.
Bytes Recv	Number of bytes received.
Decode Latency	Number of milliseconds for decoder latency.
Jitter	Number of milliseconds for receiver jitter.
Round Trip Delay	Number of milliseconds for delay.
Packets Lost	Number of packets lost.
Packet Error	Number of invalid packets received.
Mapped RTP Port	The port mapped for Real Time Protocol traffic for the call.
Media Loopback	If the call is a loopback call, displays the loopback mode (source or mirror) and type (media or packet). If the call is not loopback, the field appears blank.
Loss Rate	The fraction of RTP data packets from the source lost since the beginning of reception. Defined in RFC 3611—RTP Control Protocol Extended Reports (RTCP XR).
Discard Rate	The fraction of RTP data packets from the source that have been discarded since the beginning of reception, due to late or early arrival, under-run or overflow at the receiving jitter buffer. Defined in RFC 3611—RTP Control Protocol Extended Reports (RTCP XR).
Burst Duration	The mean duration, expressed in milliseconds, of the burst periods that have occurred since the beginning of reception. Defined in RFC 3611—RTP Control Protocol Extended Reports (RTCP XR).
Gap Duration	The mean duration, expressed in milliseconds, of the gap periods that have occurred since the beginning of reception. Defined in RFC 3611—RTP Control Protocol Extended Reports (RTCP XR).

Parameter	Description
R Factor	Voice quality metric describing the segment of the call that is carried over this RTP session. Defined in RFC 3611—RTP Control Protocol Extended Reports (RTCP XR).
MOS-LQ	The estimated mean opinion score for listening quality (MOS-LQ) is a voice quality metric on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable. Defined in RFC 3611—RTP Control Protocol Extended Reports (RTCP XR).
MOS-CQ	The estimated mean opinion score for conversational quality (MOS-CQ) is defined as including the effects of delay and other effects that would affect conversational quality. Defined in RFC 3611—RTP Control Protocol Extended Reports (RTCP XR).

Downloaded Ring Tone

Parameter	Description
Status	Indicates whether the phone is downloading a ring tone (and from where) or if it is idle.
Ring Tone 1	Information about the user downloaded ring tone 1: name, size, and time-stamp of the tone.
Ring Tone 2	Information about the user downloaded ring tone 2: name, size, and time-stamp of the tone.

System Tab

This section describes the fields for the following headings on the System tab:

- **System Configuration, page 205**
- **Internet Connection Type and Static IP Settings, page 206**
- **PPPoE Settings, page 207**
- **Optional Network Configuration, page 207**

- VLAN Settings, page 209
- Wi-Fi Settings (Cisco SPA 525G only), page 210
- Bluetooth Settings (Cisco SPA 525G only), page 210
- VPN Settings, page 210

System Configuration

Parameter	Description
Restricted Access Domains (SIP)	This feature is used when implementing software customization.
Enable Web Server	Enable/disable web server of the IP phone. Defaults to yes.
Web Server Port	Port number of the web user interface. Defaults to 80.
SPA525-http-write (SPCP)	Allow Cisco Configuration Assistant (CCA) or other application to write XML file parameters directly to the phone using HTTP. Choose **yes** to allow this feature, or no to disable this feature.
Enable Web Admin Access	Lets you enable or disable local access to the web user interface. Select yes or no from the drop-down menu. Defaults to yes.
Admin Passwd	Password for the administrator. Defaults to no password.
User Password	Password for the user. Defaults to no password.

Parameter	Description
SPA525-protocol (Cisco SPA 525G only)	Allows you to choose the type of protocol for the phone: ▪ SIP—Session Initiation Protocol. Choose if the phone is used with a SIP call control system, such as the Cisco SPA 9000 or a SIP call control system from another provider such as BroadSoft or Asterisk. ▪ SPCP—Smart Phone Control Protocol. Choose if the phone is used with a Cisco Unified Communications Series server, such as the Cisco Unified Communications 500 Series for Small Business.
SPA525-auto-detect-sccp (Cisco SPA 525G only)	Choose if the phone should automatically detect the type of protocol used on the network to which it is connected. If set to yes, the phone automatically discovers if it is connected to a call control system using SPCP.
SPA525-readonly	If set to **yes**, the Signaling Protocol and Auto Detect SCCP Settings on the phone are read only. If set to **no**, the above settings on the phone can be changed by the end user.

Internet Connection Type and Static IP Settings

Parameter	Description
Internet Connection Type	Choose the type of internet connection: ▪ DHCP ▪ Static IP ▪ PPPoE (not applicable to WIP310)
Static IP	If static IP was chosen as the type of internet connection, displays the static IP address assigned to the phone.
Netmask	If static IP was chosen as the type
Gateway	Default router IP address. Blank if DHCP assigned.

Parameter	Description
LAN MTU	LAN Maximum Transmission Unit size. Default value: 1500.
Ethernet MTU (SPCP)	Ethernet Maximum Transmission Unit size. Default value: 1500.
Duplex Mode	Duplex Mode—Choose one of the following to configure the speed/duplex for the phone's Ethernet ports: ▪ Auto ▪ 10MBps/Duplex ▪ 10MBps/Half ▪ 100Mbps/Duplex ▪ 100MBps/Half

PPPoE Settings

Parameter	Description
PPPoE Login Name	Specifies the account name assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.
PPPoE Login Password	Specifies the password assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.
PPPoE Service Name	Specifies the service name assigned by the ISP for connecting on a Point-to-Point Protocol over Ethernet (PPPoE) link.

Optional Network Configuration

Parameter	Description
Host Name	The host name of the IP phone.

Parameter	Description
Domain	The network domain of the IP phone.
Primary DNS	DNS server used by IP phone in addition to DHCP supplied DNS servers if DHCP is enabled; when DHCP is disabled, this is the primary DNS server. Defaults to 0.0.0.0.
Secondary DNS	DNS server used by IP phone in addition to DHCP supplied DNS servers if DHCP is enabled; when DHCP is disabled, this is the secondary DNS server. Defaults to 0.0.0.0.
DNS Server Order	Specifies the method for selecting the DNS server. The options are Manual, Manual/DHCP, and DHCP/Manual.
DNS Query Mode	Do parallel or sequential DNS Query. With parallel DNS query mode, the IP phone sends the same request to all the DNS servers at the same time when doing a DNS lookup, the first incoming reply is accepted by the IP phone. Defaults to parallel.
Syslog Server	Specify the syslog server name and port. This feature specifies the server for logging IP phone system information and critical events. If both Debug Server and Syslog Server are specified, Syslog messages are also logged to the Debug Server.
Debug Server	The debug server name and port. This feature specifies the server for logging IP phone debug information. The level of detailed output depends on the debug level parameter setting.
Debug Level	The debug level from 0-3. The higher the level, the more debug information is generated. Zero (0) means no debug information is generated. To log SIP messages, you must set the Debug Level to at least 2. Defaults to 0.
Primary NTP Server	IP address or name of primary NTP server.
Secondary NTP Server	IP address or name of secondary NTP server.

Parameter	Description
Enable Bonjour	Enable Bonjour networking that is used by Office Manager and Cisco Configuration Assistant to discover the Cisco IP phones. Choose **yes** to enable or **no** to disable.

VLAN Settings

NOTE Not applicable to the WIP310.

Parameter	Description
Enable VLAN	Choose **Yes** to enable VLAN. Choose **no** to disable.
Enable CDP	*Enable CDP* only if you are using a switch that has Cisco Discovery Protocol. CDP is negotiation based and determines which VLAN the IP phone resides in.
VLAN ID	If you use a VLAN without CDP (VLAN enabled and CDP disabled), enter a *VLAN ID* for the IP phone. Note that only voice packets are tagged with the VLAN ID.
Enable PC Port VLAN Tagging	Enables VLAN and priority tagging on the phone data port (802.1p/q). This feature facilities tagging of the VLAN ID (802.1Q) and priority bits (802.1p) of the traffic coming from the PC port of the IP phone. Defaults to No. Choose **Yes** to enable the tagging algorithm.
PC Port VLAN Highest Priority	0-7 (default 0). The priority applied to all frames, tagged and untagged. The phone modifies the frame priority only if the incoming frame priority is higher than this value.
PC Port VLAN ID	0-4095 (default 0). Value of the VLAN ID. The phone tags all the untagged frames coming from the PC (it will not tag frames with an existing tag).

Wi-Fi Settings (Cisco SPA 525G only)

Parameter	Description
SPA525-wifi-on	Set to yes to enable Wireless-G service on the Cisco SPA 525G.

Bluetooth Settings (Cisco SPA 525G only)

Parameter	Description
Enable BT	Set to yes to enable support for Bluetooth devices on the Cisco SPA 525G.

VPN Settings

Parameter	Description
VPN Server	The IP address of the VPN server to which the phone connects.
VPN User Name	Username configured on the VPN server for the phone.
VPN Password	Password associated with the username configured on the VPN for the phone.
VPN Tunnel Group	(Optional) The tunnel group, if required by the VPN server.
Connect on Bootup	If the phone should attempt to connect to the VPN each time it is powered on. Choose **yes** to have the phone try to automatically connect, or no to keep the default behavior.

SIP Tab

This section describes the fields for the following headings on the SIP tab:

SIP Parameters

Parameter	Description
Max Forward	SIP Max Forward value, which can range from 1 to 255. Defaults to 70.
Max Redirection	Number of times an invite can be redirected to avoid an infinite loop. Defaults to 5.
Max Auth	Maximum number of times (from 0 to 255) a request may be challenged. Defaults to 2.
SIP User Agent Name	Used in outbound REGISTER requests. Defaults to $VERSION. If empty, the header is not included. Macro expansion of $A to $D corresponding to GPP_A to GPP_D allowed.
SIP Server Name	Server header used in responses to inbound responses. Defaults to $VERSION.

Parameter	Description
SIP Reg User Agent Name	User-Agent name to be used in a REGISTER request. If this is not specified, the <SIP User Agent Name> is also used for the REGISTER request. Defaults to blank.
SIP Accept Language	Accept-Language header used. To access, click the SIP tab, and fill in the SIP Accept Language field. There is no default (this indicates IP phone does not include this header). If empty, the header is not included.
DTMF Relay MIME Type	MIME Type used in a SIP INFO message to signal a DTMF event. This field must match that of the Service Provider. Defaults to application/dtmf-relay.
Hook Flash MIME Type	MIME Type used in a SIP INFO message to signal a hook flash event. The default is application/hook-flash.
Remove Last Reg	Lets you remove the last registration before registering a new one if the value is different. Select yes or no from the drop-down menu. Defaults to no.
Use Compact Header	Lets you use compact SIP headers in outbound SIP messages. Select yes or no from the drop-down menu. If set to yes, the phone uses compact SIP headers in outbound SIP messages. If set to no, the phone uses normal SIP headers. If inbound SIP requests contain compact headers, the phone reuses the same compact headers when generating the response regardless the settings of the <Use Compact Header> parameter. If inbound SIP requests contain normal headers, the phone substitutes those headers with compact headers (if defined by RFC 261) if <Use Compact Header> parameter is set to yes. Default: no

Parameter	Description
Escape Display Name	Lets you keep the Display Name private. Select yes if you want the IP phone to enclose the string (configured in the Display Name) in a pair of double quotes for outbound SIP messages. Any occurrences of or \ in the string is escaped with \ and \\ inside the pair of double quotes. Otherwise, select no. Defaults to yes.
SIP-B Enable	Enables BroadSoft call features.
Talk Package	Enables support for the BroadSoft Talk Package, which enables a user to answer or resume a call by clicking a button in an external application.
Hold Package	Enables support for the BroadSoft Hold Package, which enables a user to place a call on hold by clicking a button in an external application.
Conference Package	Enables support for the BroadSoft Conference Package, which enables a user to start a conference by clicking a button in an external application.
Notify Conference	If enabled, the unit will send out a NOTIFY with event=conference when starting a conference.
RFC 2543 Call Hold	If set to yes, unit will include c=0.0.0.0 syntax in SDP when sending a SIP re-INVITE to the peer to hold the call. If set to no, unit will not include the c=0.0.0.0 syntax in the SDP. The unit will always include a=sendonly syntax in the SDP in either case. Defaults to yes.
Random REG CID On Reboot	If set to yes, the Cisco IP phone uses a different random call-ID for registration after the next software reboot. If set to no, the Cisco IP phone tries to use the same call-ID for registration after the next software reboot. The Cisco IP phone always uses a new random Call-ID for registration after a power-cycle, regardless of this setting. Defaults to no.

Parameter	Description
Mark All AVT packets	If set to yes, all audio video transport (AVT) tone packets (encoded for redundancy) have the marker bit set. If set to no, only the first packet has the marker bit set for each DTMF event. Defaults to yes.
SIP TCP Port Min	Specifies the lowest TCP port number that can be used for SIP sessions. Defaults to 5060.
SIP TCP Port Max	Specifies the highest TCP port number that can be used for SIP sessions. Defaults to 5080.
CTI Enable	The CTI interface allows a third-party application to control and monitor the state of a phone that has registered with the Cisco SPA 9000. With this interface, an application can control a phone to initiate an outgoing call or answer an incoming call with a mouse click from a PC.
Caller ID Header	Provides the option to take the caller ID from PAID-RPID-FROM, P-ASSERTEDIDENTITY, REMOTE-PARTY-ID, or FROM header.
SRTP Method	Selects the method to use for SRTP. Two choices are available: ▪ x-sipura—legacy SRPT method ▪ s-descriptor—new method compliant with RFC-3711 and RFC-4568 The default value is "x-sipura." **NOTE** Not applicable to WIP310.
Hold Target Before REFER	Controls whether to hold call leg with transfer target before sending REFER to the transferee when initiating a fully-attended call transfer (where the transfer target has answered). Default value is "no," where the call leg is not held. **NOTE** Not applicable to WIP310.

SIP Timer Values (sec)

Parameter	Description
SIP T1	RFC 3261 T1 value (RTT estimate), which can range from 0 to 64 seconds. Defaults to .5 seconds.
SIP T2	RFC 3261 T2 value (maximum retransmit interval for non-INVITE requests and INVITE responses), which can range from 0 to 64 seconds. Defaults to 4 seconds.
SIP T4	RFC 3261 T4 value (maximum duration a message remains in the network), which can range from 0 to 64 seconds. Defaults to 5 seconds.
SIP Timer B	INVITE time-out value, which can range from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer F	Non-INVITE time-out value, which can range from 0 to 64 seconds.Defaults to 16 seconds.
SIP Timer H	INVITE final response, time-out value, which can range from 0 to 64 seconds.Defaults to 16 seconds.
SIP Timer D	ACK hang-around time, which can range from 0 to 64 seconds. Defaults to 16 seconds.
SIP Timer J	Non-INVITE response hang-around time, which can range from 0 to 64 seconds. Defaults to 16 seconds.
INVITE Expires	INVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 240 seconds.
RelNVITE Expires	RelNVITE request Expires header value. If you enter 0, the Expires header is not included in the request. Ranges from 0 to 19999999999999999999999999999999. Defaults to 30
Reg Min Expires	Minimum registration expiration time allowed from the proxy in the Expires header or as a Contact header parameter. If the proxy returns a value less than this setting, the minimum value is used. Defaults to 1 second.

Parameter	Description
Reg Max Expires	Maximum registration expiration time allowed from the proxy in the Min-Expires header. If the value is larger than this setting, the maximum value is used. Defaults to 7200.
Reg Retry Intvl (See note below)	Interval to wait before the IP phone retries registration after failing during the last registration. Defaults to 30.
Reg Retry Long Intvl (See note below)	When registration fails with a SIP response code that does not match<Retry Reg RSC>, the IP phone waits for the specified length of time before retrying. If this interval is 0, the IP phone stops trying. This value should be much larger than the Reg Retry Intvl value, which should not be 0. Defaults to 1200.
Reg Retry Random Delay	Random delay range (in seconds) to add to <Register Retry Intvl> when retrying REGISTER after a failure. This feature was added in Release 5.1. Defaults to blank, which disables this feature.
Reg Retry Long Random Delay	Random delay range (in seconds) to add to <Register Retry Long Intvl> when retrying REGSITER after a failure. This feature was added in Release 5.1. Defaults to blank, which disables this feature.
Reg Retry Intvl Cap	The maximum value to cap the exponential back-off retry delay (which starts at <Register Retry Intvl> and doubles on every REGISTER retry after a failure). In other words, the retry interval is always at <Register Retry Intvl> seconds after a failure. If this feature is enabled, <Reg Retry Random Delay> is added on top of the exponential back-off adjusted delay value. This feature was added in Release 5.1. Defaults to blank, which disables the exponential back-off feature.
Sub Min Expires	This value sets the lower limit of the REGISTER expires value returned from the Proxy server.
Sub Max Expires	This value sets the upper limit of the REGISTER min-expires value returned from the Proxy server in the Min-Expires header. Defaults to 7200.

Parameter	Description
Sub Retry Intvl	This value (in seconds) determines the retry interval when the last Subscribe request fails. Defaults to 10.

NOTE Cisco IP phones can use a RETRY-AFTER value when received from a SIP proxy server that is too busy to process a request (503 Service Unavailable message). If the response message includes a RETRY-AFTER header, the phone waits for the specified length of time before retrying to REGISTER again. If a RETRY-AFTER header is not present, the phone waits for the value specified in the *Reg Retry Interval* or the *Reg Retry Long Interval* parameter.

Response Status Code Handling

Parameter	Description
SIT1 RSC	SIP response status code for the appropriate Special Information Tone (SIT). For example, if you set the SIT1 RSC to 404, when the user makes a call and a failure code of 404 is returned, the SIT1 tone is played. Reorder or Busy Tone is played by default for all unsuccessful response status code for SIT 1 RSC through SIT 4 RSC. Defaults to blank.
SIT2 RSC	SIP response status code to INVITE on which to play the SIT2 Tone. Defaults to blank.
SIT3 RSC	SIP response status code to INVITE on which to play the SIT3 Tone. Defaults to blank.
SIT4 RSC	SIP response status code to INVITE on which to play the SIT4 Tone. Defaults to blank.
Try Backup RSC	SIP response code that retries a backup server for the current request. Defaults to blank.

Parameter	Description
Retry Reg RSC	Interval to wait before the IP phone retries registration after failing during the last registration. Defaults to blank.

RTP Parameters

Parameter	Description
RTP Port Min	Minimum port number for RTP transmission and reception. Minimum port number for RTP transmission and reception. Should define a range that contains at least 10 even number ports (twice the number of lines); for example, configure RTP port min to 16384 and RTP port max to 16402. Defaults to 16384.
RTP Port Max	Maximum port number for RTP transmission and reception. Should define a range that contains at least 10 even number ports (twice the number of lines); for example, configure RTP port min to 16384 and RTP port max to 16402. Defaults to 16482.
RTP Packet Size	Packet size in seconds, which can range from 0.01 to 0.16. Valid values must be a multiple of 0.01 seconds. Defaults to 0.030.
Max RTP ICMP Err	Number of successive ICMP errors allowed when transmitting RTP packets to the peer before the IP phone terminates the call. If value is set to 0, the IP phone ignores the limit on ICMP errors. Defaults to 0.

Parameter	Description
RTCP Tx Interval	Interval for sending out RTCP sender reports on an active connection. It can range from 0 to 255 seconds. During an active connection, the IP phone can be programmed to send out compound RTCP packet on the connection. Each compound RTP packet except the last one contains a SR (Sender Report) and a SDES (Source Description). The last RTCP packet contains an additional BYE packet. Each SR except the last one contains exactly 1 RR (Receiver Report); the last SR carries no RR. The SDES contains CNAME, NAME, and TOOL identifiers. The CNAME is set to <User ID>@<Proxy>, NAME is set to <Display Name> (or Anonymous if user blocks caller ID), and TOOL is set to the Vendor/Hardware-platform-software-version (such as Cisco/IP phone-1.0.3 1(b)). The NTP timestamp used in the SR is a snapshot of the IP phone's local time, not the time reported by an NTP server. If the IP phone receives a RR from the peer, it attempts to compute the round trip delay and show it as the <Call Round Trip Delay> value (ms) in the Info section of IP phone web page. Defaults to 0.
No UDP Checksum	Select yes if you want the IP phone to calculate the UDP header checksum for SIP messages. Otherwise, select no. Defaults to no.
Symmetric RTP	Enable symmetric RTP operation. If enabled, sends RTP packets to the source address and port of the last received valid inbound RTP packet. If disabled (or before the first RTP packet arrives) sends RTP to the destination as indicated in the inbound SDP. Defaults to no.

Parameter	Description
Stats In BYE	Determines whether the IP phone includes the P-RTP-Stat header or response to a BYE message. The header contains the RTP statistics of the current call. Select yes or no from the drop-down menu. The format of the P-RTP-Stat header is: P-RTP-State: PS=<packets sent>,OS=<octets sent>,PR=<packets received>,OR=<octets received>,PL=<packets lost>,JI=<jitter in ms>,LA=<delay in ms>,DU=<call duration in s>,EN=<encoder>,DE=<decoder>. Defaults to no.

SDP Payload Types

The configured dynamic payloads are used for outbound calls only where the IP phone presents the SDP offer. For inbound calls with a SDP offer, the IP phone follows the caller dynamic payload type assignments.

The IP phone uses the configured codec names in its outbound SDP. The IP phone ignores the codec names in incoming SDP for standard payload types (0 – 95). For dynamic payload types, the IP phone identifies the codec by the configured codec names. Comparison is case-insensitive.

Parameter	Description
AVT Dynamic Payload	AVT dynamic payload type. Ranges from 96-127. Defaults to 101.
INFOREQ Dynamic Payload	INFOREQ dynamic payload type. Defaults to blank.
G726r16 Dynamic Payload	G.726-16 dynamic payload type. Ranges from 96-127. Defaults to 98. **NOTE** Not applicable to Cisco SPA 525G/WIP310.
G726r24 Dynamic Payload	G.726-24 dynamic payload type. Ranges from 96-127. Defaults to 97. **NOTE** Not applicable to Cisco SPA 525G/WIP310.

Parameter	Description
G726r32 Dynamic Payload	G726r32 dynamic payload type. The default is 2.
G726r40 Dynamic Payload	G.726-40 dynamic payload type. Ranges from 96-127. Defaults to 96. **NOTE** Not applicable to Cisco SPA 525G/WIP310.
G729b Dynamic Payload	G729b Dynamic Payload type. Defaults to 99.
EncapRTP Dynamic Payload	EncapRTP Dynamic Payload type. Defaults to 112.
RTP-Start-Loopback Dynamic	RTP-Start-Loopback Dynamic Payload. Defaults to 113.
RTP-Start-Loopback Codec	RTP-Start-Loopback Codec. Select one of following: G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a, or G723. Cisco SPA 525G choices: G711u, G711a, G726-32, G729a, G722. Defaults to G711u.
AVT Codec Name	AVT codec name used in SDP. Defaults to telephone-event.
G711u Codec Name	G.711u codec name used in SDP. Defaults to PCMU.
G711a Codec Name	G.711a codec name used in SDP. Defaults to PCMA.
G726r16 Codec Name	G.726-16 codec name used in SDP. Defaults to G726-16. **NOTE** Not applicable to Cisco SPA 525G/WIP310.

Parameter	Description
G726r24 Codec Name	G.726-24 codec name used in SDP. Defaults to G726-24. **NOTE** Not applicable to Cisco SPA 525G/WIP310.
G726r32 Codec Name	G.726-32 codec name used in SDP. Defaults to G726-32.
G726r40 Codec Name	G.726-40 codec name used in SDP. Defaults to G726-40. **NOTE** Not applicable to Cisco SPA 525G/WIP310.
G729a Codec Name	G.729a codec name used in SDP. Defaults to G729a.
G729b Codec Name	G.729b codec name used in SDP. Defaults to G729ab.
G729a Codec Name	G.729a codec name used in SDP. Defaults to G729a.
G722 Codec Name	G.722 codec name used in SDP. Defaults to G722. **NOTE** Not supported on the WIP310.
EncapRTP Codec Name	EncapRTP codec name used in SDP. Defaults to encaprtp.

NAT Support Parameters

Parameter	Description
Handle VIA received	If you select yes, the phone processes the received parameter in the VIA header (this is inserted by the server in a response to any of its requests). If you select no, the parameter is ignored. Select yes or no from the drop-down menu. Defaults to no.
Handle VIA rport	If you select yes, the IP phone processes the rport parameter in the VIA header (this is inserted by the server in a response to any of its requests). If you select no, the parameter is ignored. Select yes or no from the drop-down menu. Defaults to no.
Insert VIA received	Inserts the received parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Select yes or no from the drop-down menu. Defaults to no.
Insert VIA rport	Inserts the rport parameter into the VIA header of SIP responses if the received-from IP and VIA sent-by IP values differ. Select yes or no from the drop-down menu. Defaults to no.
Substitute VIA Addr	Lets you use NAT-mapped IP:port values in the VIA header. Select yes or no from the drop-down menu. Defaults to no.
Send Resp To Src Port	Sends responses to the request source port instead of the VIA sent-by port. Select yes or no from the drop-down menu. Defaults to no.
STUN Enable	Enables the use of STUN to discover NAT mapping. Select yes or no from the drop-down menu. Defaults to no.

Parameter	Description
STUN Test Enable	If the STUN Enable feature is enabled and a valid STUN server is available, the IP phone can perform a NAT-type discovery operation when it powers on. It contacts the configured STUN server, and the result of the discovery is reported in a Warning header in all subsequent REGISTER requests. If the IP phone detects symmetric NAT or a symmetric firewall, NAT mapping is disabled. Defaults to no.
STUN Server	IP address or fully-qualified domain name of the STUN server to contact for NAT mapping discovery. You can use a public STUN server or set up your own STUN server.
EXT IP	External IP address to substitute for the actual IP address of the IP phone in all outgoing SIP messages. If 0.0.0.0 is specified, no IP address substitution is performed. If this parameter is specified, the IP phone assumes this IP address when generating SIP messages and SDP (if NAT Mapping is enabled for that line). However, the results of STUN and VIA received parameter processing, if available, supersede this statically configured value. Defaults to blank.
EXT RTP Port Min	External port mapping number of the RTP Port Min. number. If this value is not zero, the RTP port number in all outgoing SIP messages is substituted for the corresponding port value in the external RTP port range. Defaults to blank.
NAT Keep Alive Intvl	Interval between NAT-mapping keep alive messages. Defaults to 15.

Linksys Key System Parameters

Parameter	Description
Linksys Key System	Enable or disable the Linksys Key System on the IP phone. Defaults to yes.
Multicast Address	The multicast address is used by the Cisco SPA 9000 to communicate with the Cisco SPA IP phones. Defaults to 224.168.168.168:6061.
Key System Auto Discovery	Enables or disables auto discovery of the call control server (for example, the Cisco SPA 9000). Disable this feature for teleworkers or other scenarios where multicast does not work.
Key System IP Address	IP address of the call control server IP. Enter the IP address for teleworkers or other scenarios where multicast does not work.
Force LAN Codec	The choices are: none, G.711u, or G.711a. Defaults to none.

Provisioning Tab

NOTE For information about the Provisioning page, see the *Cisco Small Business IP Telephony Devices Provisioning Guide*.

Regional Tab

This section describes the fields for the following headings on the Regional tab:

- **Call Progress Tones, page 226**
- **Distinctive Ring Patterns, page 229**

Call Progress Tones

Parameter	Description
Dial Tone	Prompts the user to enter a phone number. Defaults to 350@-19,440@-19;10(*/0/1+2).
Bluetooth Dial Tone (Cisco SPA 525G only)	Tone that indicates a bluetooth headset is on and the user can make a call. Defaults to 350@-19,440@-19;1(0/*/0);10(*/0/1+2).
Outside Dial Tone	Alternative to the Dial Tone. It prompts the user to enter an external phone number, as opposed to an internal extension. It is triggered by a, (comma) character encountered in the dial plan. Defaults to 420@-16;10(*/0/1).
Prompt Tone	Prompts the user to enter a call forwarding phone number. Defaults to 520@-19,620@-19;10(*/0/1+2).
Busy Tone	Played when a 486 RSC is received for an outbound call. Defaults to 480@-19,620@-19;10(.5/.5/1+2).

Parameter	Description
Reorder Tone	Played when an outbound call has failed or after the far end hangs up during an established call. Reorder Tone is played automatically when <Dial Tone> or any of its alternatives times out. Defaults to 480@-19,620@-19;10(.25/.25/1+2).
Off Hook Warning Tone	Played when the caller has not properly placed the handset on the cradle. Off Hook Warning Tone is played when Reorder Tone times out. Defaults to 480@10,620@0;10(.125/.125/1+2).
Ring Back Tone	Played during an outbound call when the far end is ringing. Defaults to 440@-19,480@-19;*(2/4/1+2).
Call Waiting Tone	Played when a call is waiting. Defaults to 440@-10;30(.3/9.7/1)
Confirm Tone	Brief tone to notify the user that the last input value has been accepted. Defaults to 600@-16; 1(.25/.25/1).
SIT1 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. Defaults to 985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0).
SIT2 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. Defaults to 914@-16,1371@-16,1777@-16;20(.274/0/1,.274/0/2,.380/0/3,0/4/0).
SIT3 Tone	Alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. Defaults to 914@-16,1371@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0)

Parameter	Description
SIT4 Tone	This is an alternative to the Reorder Tone played when an error occurs as a caller makes an outbound call. The RSC to trigger this tone is configurable on the SIP screen. Defaults to 985@-16,1371@-16,1777@-16;20(.380/0/1,.274/0/2,.380/0/3,0/4/0).
MWI Dial Tone	Played instead of the Dial Tone when there are unheard messages in the caller's mailbox. Defaults to 350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2).
Cfwd Dial Tone	Played when all calls are forwarded. Defaults to 350@-19,440@-19;2(.2/.2/1+2);10(*/0/1+2).
Holding Tone	Informs the local caller that the far end has placed the call on hold. Defaults to 600@-19*(.1/.1/1,.1/.1/1,.1/9.5/1).
Conference Tone	Played to all parties when a three-way conference call is in progress. Defaults to 350@-19;20(.1/.1/1,.1/9.7/1).
Secure Call Indication Tone	Played when a call has been successfully switched to secure mode. It should be played only for a short while (less than 30 seconds) and at a reduced level (less than -19 dBm) so it does not interfere with the conversation. Defaults to 397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2).
Page Tone	Specifies the tone transmitted when the paging feature is enabled. Defaults to 600@-16;.3(.05/0.05/1).
Alert Tone	Played when an alert occurs. Defaults to 600@-19;.2(.05/0.05/1).
System Beep	Audible notification tone played when a system error occurs. Defaults to 600@-16;.1(.05/0.05/1). **NOTE** WIP310 and Cisco SPA 525G only.

Distinctive Ring Patterns

Parameter	Description
Cadence 1	Cadence script for distinctive ring 1. Defaults to 60(2/4).
Cadence 2	Cadence script for distinctive ring 2. Defaults to 60(.3/.2, 1/.2,.3/4.
Cadence 3	Cadence script for distinctive ring 3. Defaults to 60(.8/.4,.8/4).
Cadence 4	Cadence script for distinctive ring 4. Defaults to 60(.4/.2,.3/.2,.8/4).
Cadence 5	Cadence script for distinctive ring 5. Defaults to 60(.2/.2,.2/.2,.2/.2,1/4)
Cadence 6	Cadence script for distinctive ring 6. Defaults to60(.2/.4,.2/.4,.2/4).
Cadence 7	Cadence script for distinctive ring 7. Defaults to 60(4.5/4).
Cadence 8	Cadence script for distinctive ring 8. Defaults to 60(0.25/9.75)
Cadence 9	Cadence script for distinctive ring 9. Defaults to 60(.4/.2,.4/2).

Control Timer Values (sec)

Parameter	Description
Reorder Delay	Delay after far end hangs up before reorder tone is played. 0 = plays immediately, inf = never plays. Range: 0–255 seconds. Defaults to 5.
Call Back Expires	Expiration time in seconds of a call back activation. Range: 0–65535 seconds. Defaults to 1800.
Call Back Retry Intvl	Call back retry interval in seconds. Range: 0–255 seconds. Defaults to 30.
Call Back Delay	Delay after receiving the first SIP 18x response before declaring the remote end is ringing. If a busy response is received during this time, the IP phone still considers the call as failed and keeps on retrying. Defaults to 0.5.
Interdigit Long Timer	Long timeout between entering digits when dialing. The interdigit timer values are used as defaults when dialing. The Interdigit_Long_Timer is used after any one digit, if all valid matching sequences in the dial plan are incomplete as dialed. Range: 0–64 seconds. Defaults to 10.
Interdigit Short Timer	Short timeout between entering digits when dialing. The Interdigit_Short_Timer is used after any one digit, if at least one matching sequence is complete as dialed, but more dialed digits would match other as yet incomplete sequences. Range: 0–64 seconds. Defaults to 3.

Vertical Service Activation Codes

The following Vertical Service Activation Codes are automatically appended to the dial plan.

Parameter	Description
Call Return Code	This code calls the last caller. Defaults to *69.
Blind Transfer Code	Begins a blind transfer of the current call to the extension specified after the activation code. Defaults to *98.
Call Back Act Code	Starts a callback when the last outbound call is not busy. Defaults to *66.
Call Back Deact Code	Cancels a callback. Defaults to *86.
Cfwd All Act Code	Forwards all calls to the extension specified after the activation code. Defaults to *72.
Cfwd All Deact Code	Cancels call forwarding of all calls. Defaults to *73.
Cfwd Busy Act Code	Forwards busy calls to the extension specified after the activation code. Defaults to *90.
Cfwd Busy Deact Code	Cancels call forwarding of busy calls. Defaults to *91.
Cfwd No Ans Act Code	Forwards no-answer calls to the extension specified after the activation code. Defaults to *92.
Cfwd No Ans Deact Code	Cancels call forwarding of no-answer calls. Defaults to *93.
CW Act Code	Enables call waiting on all calls. Defaults to *56.

Parameter	Description
CW Deact Code	Disables call waiting on all calls. Defaults to *57.
CW Per Call Act Code	Enables call waiting for the next call. Defaults to *71.
CW Per Call Deact Code	Disables call waiting for the next call. Defaults to *70.
Block CID Act Code	Blocks caller ID on all outbound calls. Defaults to *67.
Block CID Deact Code	Removes caller ID blocking on all outbound calls. Defaults to *68.
Block CID Per Call Act Code	Blocks caller ID on the next outbound call. Defaults to *81.
Block CID Per Call Deact Code	Removes caller ID blocking on the next inbound call. Defaults to *82.
Block ANC Act Code	Blocks all anonymous calls. Defaults to *77.
Block ANC Deact Code	Removes blocking of all anonymous calls. Defaults to *87.
DND Act Code	Enables the do not disturb feature. Defaults to *78.
DND Deact Code	Disables the do not disturb feature. Defaults to *79.
Secure All Call Act Code	Makes all outbound calls secure. Defaults to *16.
Secure No Call Act Code	Makes all outbound calls not secure. Defaults to *17.

Parameter	Description
Secure One Call Act Code	Makes the next outbound call secure. (It is redundant if all outbound calls are secure by default.) Defaults to *18.
Secure One Call Deact Code	Makes the next outbound call not secure. (It is redundant if all outbound calls are not secure by default.) Defaults to *19.
Paging Code	The star code used for paging the other clients in the group. Defaults to *96.
Call Park Code	The star code used for parking the current call. Defaults to *38.
Call Pickup Code	The star code used for picking up a ringing call. Defaults to *36.
Call UnPark Code	The star code used for picking up a call from the call park. Defaults to *39.
Group Call Pickup Code	The star code used for picking up a group call. Defaults to *37.
Media Loopback Code	The star code used for media loopback. Defaults to *03.

Parameter	Description
Referral Services Codes	These codes tell the IP phone what to do when the user places the current call on hold and is listening to the second dial tone. One or more *code can be configured into this parameter, such as *98, or *97|*98|*123, etc. Max total length is 79 chars. This parameter applies when the user places the current call on hold (by Hook Flash) and is listening to second dial tone. Each *code (and the following valid target number according to current dial plan) entered on the second dial-tone triggers the IP phone to perform a blind transfer to a target number that is prepended by the service *code. For example, after the user dials *98, the IP phone plays a special dial tone called the Prompt Tone while waiting for the user the enter a target number (which is checked according to dial plan as in normal dialing). When a complete number is entered, the IP phone sends a blind REFER to the holding party with the Refer-To target equals to *98<target_number>. This feature allows the IP phone to hand off a call to an application server to perform further processing, such as call park. The *codes should not conflict with any of the other vertical service codes internally processed by the IP phone. You can empty the corresponding *code that you do not want to IP phone to process.

Parameter	Description
Feature Dial Services Codes	These codes tell the IP phone what to do when the user is listening to the first or second dial tone. One or more *code can be configured into this parameter, such as *72, or *72|*74|*67|*82, etc. Max total length is 79 chars. This parameter applies when the user has a dial tone (first or second dial tone). Enter *code (and the following target number according to current dial plan) entered at the dial tone triggers the IP phone to call the target number prepended by the *code. For example, after user dials *72, the IP phone plays a prompt tone awaiting the user to enter a valid target number. When a complete number is entered, the IP phone sends a INVITE to *72<target_number> as in a normal call. This feature allows the proxy to process features like call forward (*72) or BLock Caller ID (*67). The *codes should not conflict with any of the other vertical service codes internally processed by the IP phone. You can empty the corresponding *code that you do not want to IP phone to process. You can add a parameter to each *code in Features Dial Services Codes to indicate what tone to play after the *code is entered, such as *72‘c'|*67‘p‘. Below are a list of allowed tone parameters (note the use of back quotes surrounding the parameter w/o spaces) ▪ c = Cfwd Dial Tone ▪ d = Dial Tone ▪ m = MWI Dial Tone ▪ o = Outside Dial Tone ▪ p = Prompt Dial Tone ▪ s = Second Dial Tone ▪ x = No tones are place, x is any digit not used above
	If no tone parameter is specified, the IP phone plays Prompt tone by default. If the *code is not to be followed by a phone number, such as *73 to cancel call forwarding, do not include it in this parameter. In that case, simple add that *code in the dial plan and the IP phone send INVITE *73@..... as usual when user dials *73.

Vertical Service Announcement Codes

- Service Annc (Announcement) Base Number: Defaults to blank.
- Service Annc (Announcement) Extension Codes: Defaults to blank.

Outbound Call Codec Selection Codes

These codes automatically appended to the dial-plan. You do not need to include them in the dial-plan.

Parameter	Description
Prefer G711u Code	Makes this codec the preferred codec for the associated call. Defaults to *017110.
Force G711u Code	Makes this codec the only codec that can be used for the associated call. Defaults to *027110.
Prefer G711a Code	Makes this codec the preferred codec for the associated call. Defaults to *017111
Force G711a Code	Makes this codec the only codec that can be used for the associated call. Defaults to *027111.
Prefer G722 Code	Makes this codec the preferred codec for the associated call. Defaults to *01722. Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio. **NOTE** Not supported on the WIP310.

Parameter	Description
Force G722 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02722. Only one G.722 call at a time is allowed. If a conference call is placed, a SIP re-invite message is sent to switch the calls to narrowband audio. **NOTE** Not supported on the WIP310.
Prefer L16 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *01016.
Force L16 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02016.
Prefer G723 Code	Makes this codec the preferred codec for the associated call. Defaults to *01723. **NOTE** Not applicable to WIP310 or Cisco SPA 525G.
Force G723 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02723. **NOTE** Not applicable to WIP310 or Cisco SPA 525G.
Prefer G726r16 Code	Makes this codec the preferred codec for the associated call. Defaults to *0172616. **NOTE** Not applicable to WIP310 or Cisco SPA 525G.
Force G726r16 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *0272616. **NOTE** Not applicable to WIP310 or Cisco SPA 525G.

Parameter	Description
Prefer G726r24 Code	Makes this codec the preferred codec for the associated call. Defaults to *0172624. **NOTE** Not applicable to WIP310 or Cisco SPA 525G.
Force G726r24 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *0272624. **NOTE** Not applicable to WIP310 or Cisco SPA 525G.
Prefer G726r32 Code	Makes this codec the preferred codec for the associated call. Defaults to *0172632.
Force G726r32 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *0272632.
Prefer G726r40 Code	Makes this codec the preferred codec for the associated call. Defaults to *0172640. **NOTE** Not applicable to WIP310 or Cisco SPA 525G.
Force G726r40 Code	Makes this codec the only codec that can be used for the associated call. Defaults to *0272640. **NOTE** Not applicable to WIP310 or Cisco SPA 525G.
Prefer G729a Code	Makes this codec the preferred codec for the associated call. Defaults to *01729.
Force G729a Code	Makes this codec the only codec that can be used for the associated call. Defaults to *02729.

Time (Cisco SPA 525G Only)

Parameter	Description
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00,..., GMT, GMT+01:00, GMT+02:00, ..., GMT+13:00. Defaults to GMT-08:00.
Time Offset	This specifies the offset from GMT to use for the local system time.
Daylight Saving Time Rule	See "Daylight Saving Time Rule" in **Miscellaneous, page 239**.
Daylight Saving Time Enable	Select yes to enable Daylight Saving Time.

Language (Cisco SPA 525G only)

Parameter	Description
Dictionary Server Script.	See "Dictionary Server Script" in **Miscellaneous, page 239**.
Language Selection	See "Language Selection" in **Miscellaneous, page 239**.

Miscellaneous

Parameter	Description
Set Local Date (mm/dd)	Sets the local date (mm represents the month and dd represents the day). The year is optional and uses two or four digits. **NOTE** Not applicable to the Cisco SPA 525G.

Parameter	Description
Set Local Time (HH/mm)	Sets the local time (hh represents hours and mm represents minutes). Seconds are optional. **NOTE** Not applicable to the Cisco SPA 525G.
Time Zone	Selects the number of hours to add to GMT to generate the local time for caller ID generation. Choices are GMT-12:00, GMT-11:00,..., GMT, GMT+01:00, GMT+02:00, ..., GMT+13:00. Defaults to GMT-08:00. **NOTE** Found in the **Time** section for the Cisco SPA 525G.
Time Offset (HH/mm)	This specifies the offset from GMT to use for the local system time. **NOTE** Found in the **Time** section for the Cisco SPA 525G.

Parameter	Description
Daylight Saving Time Rule	Enter the rule for calculating daylight saving time; it should include the start, end, and save values. This rule is comprised of three fields. Each field is separated by ; (a semicolon) as shown below. Optional values inside [ ] (the brackets) are assumed to be 0 if they are not specified. Midnight is represented by 0:0:0 of the given date. This is the format of the rule: Start = <start-time>; end=<end-time>; save = <save-time>. The <start-time> and <end-time> values specify the start and end dates and times of daylight saving time. Each value is in this format: <month> /<day> / <weekday>[/HH:[mm[:ss]]] The <save-time> value is the number of hours, minutes, and/or seconds to add to the current time during daylight saving time. The <save-time> value can be preceded by a negative (-) sign if subtraction is desired instead of addition. The <save-time> value is in this format: [/[+|-]HH:[mm[:ss]]] The <month> value equals any value in the range 1-12 (January-December). The <day> value equals [+|-] any value in the range 1-31. If <day> is 1, it means the <weekday> on or before the end of the month (in other words the last occurrence of < weekday> in that month).

Parameter	Description
	The <weekday> value equals any value in the range 1-7 (Monday-Sunday). It can also equal 0. If the <weekday> value is 0, this means that the date to start or end daylight saving is exactly the date given. In that case, the <day> value must not be negative. If the <weekday> value is not 0 and the <day> value is positive, then daylight saving starts or ends on the <weekday> value on or after the date given. If the <weekday> value is not 0 and the <day> value is negative, then daylight saving starts or ends on the <weekday> value on or before the date given. The abbreviation HH stands for hours (0-23). The abbreviation mm stands for minutes (0-59). The abbreviation ss stands for seconds (0-59). The default Daylight Saving Time Rule is start=4/1/7;end=10/-1/7;save=1. **NOTE** Found in the **Time** section for the Cisco SPA 525G.
Daylight Savings Time Enable	Select yes to enable Daylight Saving Time. **NOTE** Found in the **Time** section for the Cisco SPA 525G.
DTMF Playback Level	Local DTMF playback level in dBm, up to one decimal place. Defaults to -16.
DTMF Playback Length	Local DTMF playback duration in milliseconds. Defaults to .1.
Inband DTMF Boost	Controls the amount of amplification applied DTMF signals. Choices are OdB, 3dB, 6dB, 9dB, 12dB, 15dB, or 18dB. Defaults to 12dB.

Parameter	Description

Dictionary Server Script/ SCCP Dictionary Server Script (Cisco SPA 525G)	Defines the location of the dictionary server, the languages available and the associated dictionary. The syntax is as follows:
	`<Dictionary_Server_Script ua="na">`
	`</Dictionary_Server_Script>`
	Defaults to blank and the maximum number of characters is 512. The detailed format is as follows:
	`serv={server ip port and root path};`
	`d0=<language0>;x0=<dictionary0 filename>;`
	`d1=<language1>;x1=<dictionary1 filename>;`
	`d2=<language2>;x2=<dictionary2 filename>;`
	`d3=<language3>;x3=<dictionary3 filename>;`
	`d4=<language4>;x4=<dictionary4 filename>;`
	`d5=<language5>;x5=<dictionary5 filename>;`
	`d6=<language6>;x6=<dictionary6 filename>;`
	`d7=<language3>;x7=<dictionary7 filename>;`
	`d8=<language8>;x8=<dictionary8 filename>;`
	`d9=<language5>;x9=<dictionary9 filename>;`

Parameter	Description

	The following is an example value:
	`<Dictionary_Server_Script ua="na">`
	`serv=tftp://192.168.1.119/ ;d0=English;x0=enS_v101.xml;d1=Spanish ;x1=esS_v101.xml </ Dictionary_Server_Script>`
	NOTE Not applicable to the WIP310.

Language Selection/SCCP Language Selection (Cisco SPA 525G)	Specifies the default language. The value needs to match one of the languages supported by the dictionary server. The script (dx value) is as follows:
	`<Language_Selection ua="na">`
	`</Language_Selection>`
	Defaults to blank and the maximum number of characters is 512. The following is an example:
	`<Language_Selection ua="na"> Spanish`
	`</Language_Selection>`
	NOTE Not applicable to the WIP310.

Default Character Encoding (Cisco SPA 5XX)	The default is ISO-8859-1 for backward compatibility with Cisco SPA900 series phones. If set to UTF-8, line keys and other labels entered via the Web Administration Interface containing UTF-8 characters will be displayed correctly on the phone. (SIP only)

Phone Tab

This section describes the fields for the following headings on the Phone tab:

General

Parameter	Description
Station Name	Name to identify this station (reserved for future use).
Voice Mail Number	Phone number or URL to check voice mail. Note that The service provider often hosts a voice mail service. The advantages of hosted voice mail include: ▪ Advanced features such as voice mail to email conversion. ▪ Calls can go to voice mail when the broadband connection is down.

Parameter	Description

Text Logo	Text logo to display when the phone boots up. A service provider, for example, can enter logo text as follows:
	▪ Up to 2 lines of text
	▪ Each line must be fewer than 32 characters
	▪ Insert a new line character (\n) between lines
	▪ Insert escape code %0a
	For example, “Super\n%0aTelecom” will display:
	`Super`
	`Telecom`
	NOTE Not applicable to the WIP310. On the Cisco SPA 525G, this setting is located in the **User** tab. See **Screen (Cisco SPA 525G), page 281**.

BMP Picture Download URL	URL locating the bitmap (.BMP) file to display on the LCD background. For more information, see the **“Configuring Phone Information and Display Settings” section on page 32**. **NOTE** Not applicable to the WIP310. On the Cisco SPA 525G, this setting is located in the **User** tab. See **Screen (Cisco SPA 525G), page 281**.
Select Logo	Select from Default, BMP Picture, Text Logo, or None. Defaults to Default. **NOTE** Not applicable to the WIP310. On the Cisco SPA 525G, this setting is located in the **User** tab. See **Screen (Cisco SPA 525G), page 281**.
Select Background Picture	Select from Default, BMP Picture, or None. Defaults to Default. **NOTE** Not applicable to the WIP310. On the Cisco SPA 525G, this setting is located in the **User** tab. See **Screen (Cisco SPA 525G), page 281**.
Softkey Labels Font	Choose the font width for the softkey labels to display on your phone. See **Customizing Phone Softkeys, page 50**.

Parameter	Description
Screen Saver Enable	Enables a screen saver on the phone's LCD. When the phone is idle for a specified time, it enters screen saver mode. (Users can set up screen savers directly using phone Setup button.) Any button press or on/off hook event triggers the phone to return to its normal mode. (The screen shows "Press any key to unlock your phone.") If a user password is set, the user must enter it to exit screen saver mode. **NOTE** Not applicable to the WIP310. Screen saver settings are found in the **User** tab on the Cisco SPA 525G.
Screen Saver Wait	Amount of idle time before screen saver displays. **NOTE** Not applicable to the WIP310. Screen saver settings are found in the **User** tab on the Cisco SPA 525G.
Screen Saver Icon	In screen saver mode, the phone LCD can display: A background picture. The station time in the middle of the screen. A moving padlock icon. When the phone is locked, the status line displays a scrolling message "Press any key to unlock your phone." A moving phone icon. The station date and time in the middle of the screen. **NOTE** Not applicable to the WIP310. Screen saver settings are found in the **User** tab on the Cisco SPA 525G.
JPEG Logo Download URL (Cisco SPA 525G)	URL from which to download a .jpg file for the phone logo display.
JPEG Wallpaper Download URL (Cisco SPA 525G)	URL from which to download a .jpg file for the phone wallpaper.
Enable SMS	Enables sending and receiving of SMS text messages on the phone. **NOTE** WIP310 only.

Line Key

When used in the configuration profile, parameters in this section must be appended with *n*, where *n* represents line 1, 2, 3, 4, 5 or 6. For more information on these parameters, see the **"Configuring Lines and Extensions" section on page 20**.

NOTE Does not apply to the WIP310.

Parameter	Description
Extension	Extension number of the line key.
Short Name	A short label shown on the LCD display for line key 1 through line key 6.
Share Call Appearance	**Yes** indicates that Line Key 1/2/3/4/5/6 is a shared call appearance. Otherwise this call appearance is not shared (it is private). Defaults to no.
Extended Function	Use to assign Busy Lamp Field, Call Pickup, and Speed Dial Functions to Idle Lines on the IP phone. Syntax is: `fnc=type;sub=stationname@$PROXY;ext=extension#@$PROXY` where: ▪ fnc: function ▪ blf: busy lamp field ▪ cp: call pickup ▪ sub: station name (not needed for speed dial) ▪ ext or usr: extension or user (the usr and ext keywords are interchangeable)

Parameter	Description
Subscribe Expires	Specifies how long the subscription remains valid. After the specified period of time, elapses, the IP phone initiates a new subscription. Defaults to 1800.
Subscribe Retry Interval	Specifies the length of time to wait to try again if subscription fails.
Subscribe Delay	Length of delay before attempting to subscribe. Defaults to 1.
Server Type	Selects the type of server used (Cisco SPA 9000, BroadSoft, or Asterisk).

Miscellaneous Line Key Settings

NOTE Does not apply to the WIP310.

Parameter	Description
SCA Line ID Mapping	Specifies the shared call appearance line ID mapping. Choose Vertical First or Horizontal First. Each LED can hold two calls and the first call on an LED makes it light up. Horizontal first means the second call makes the same LED flash. Vertical first means the second call lights up the next LED. For example, if Extension 101 is assigned to two LEDs, and Vertical First is selected, the second call on Extension 101 lights up the second LED. The third call makes the first LED flash, and the fourth call makes the second LED flash. If Horizontal First is selected, the second call on Extension 101 makes the first LED flash. The third call lights up the second LED, and the fourth call makes the second LED flash.

Parameter	Description
SCA Barge-In Enable	Enables the SCA Barge-In. Defaults to no.

Line Key LED Pattern

NOTE Does not apply to the WIP310.

Parameter	Description
Idle LED	LED pattern during the Idle state, where the call appearance is not is in use and is available to make a new call. Leaving this entry blank indicates the default value of c=g.
Remote Undefined LED	LED pattern during the Remote Undefined state, where the shared call state is undefined (the station is still waiting for the state information from the application server). Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Seized LED	LED pattern during the Local Seized state, where this station has seized the call appearance to prepare for a new outbound call. Leaving this entry blank indicates the default value of c=r.
Remote Seized LED	LED pattern during the Remote Seized state, where the shared call appearance is seized by another station. Not application if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Progressing LED	LED pattern during the Local Progressing state, where this station is attempting on this call appearance an outgoing call that is in proceeding (i.e. the called number is ringing). Leaving this entry blank indicates the default value of c=r.

Parameter	Description
Remote Progressing LED	LED pattern during the Remote Progressing state, where another station is attempting on this shared call appearance an outbound call that is progressing. Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Ringing LED	LED pattern during the Local Ringing state, when the call appearance is ringing. Leaving this entry blank indicates the default value of c=r;p=f.
Remote Ringing LED	LED pattern during the Remote Ringing state, where the shared call appearance is in ringing on another station. Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Active LED	LED pattern during the Local Active state, where the call appearance is engaged in an active call. Leaving this entry blank indicates the default value of c=r.
Remote Active LED	LED pattern during the Remote Active state, where another station is engaged in an active call on this shared call appearance. Not applicable is this call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=d.
Local Held LED	LED pattern during the Local Held state, where the call appearance is held by this station. Leaving this entry blank indicates the default value of c=r;p=s.
Remote Held LED	LED pattern during the Remote Held state, where another station has placed this call appearance on hold. Not applicable if the call appearance is not shared. Leaving this entry blank indicates the default value of c=4,p=s.
Register Failed LED	LED pattern when the corresponding extension has failed to register with the proxy server. Leaving this entry blank indicates the default value of c=a.
Disabled LED	LED pattern when the Call Appearance is disabled (not available for any incoming or outgoing call). Leaving this entry blank indicates the default value of c=o.
Registering LED	LED Pattern when the corresponding extension is trying to register with the proxy server. Leaving this entry blank indicates the default value of c=r;p=s.

Parameter	Description
Call Back Active LED	Call Back operation is currently active on this call appearance is not shared. Leaving this entry blank indicates the default value of c=r;p=s.
Trunk In-Use LED	LED pattern that indicates that a shared trunk is in use.
Trunk No Service LED	LED pattern that indicates that a shared trunk is not in service.
Trunk Reserved LED	LED pattern to indicate that a shared trunk has been reserved.

Supplementary Services

Enable or disable the corresponding supplementary services on the phone. A value of “yes” indicates enabled; “no” indicates disabled.

Parameter	Description
Conference Serv	Enable/disable Three way conference service. Defaults to yes.
Attn Transfer Serv	Enable/disable attended-call-transfer service. Defaults to yes.
Blind Transfer Serv	Enable/disable blind-call-transfer service. Defaults to yes.
DND Serv	Enable/disable do-not-disturb service. Defaults to yes.
Block ANC Serv	Enable/disable block-anonymous-call service. Defaults to yes.
Call Back Serv	Enable/disable call-back (a.k.a. repeating dialing) service. Defaults to yes.

Parameter	Description
Block CID Serv	Enable/disable blocking outbound Caller-ID service. Defaults to yes.
Secure Call Serv	Enable/disable secure-call service. Defaults to yes.
Cfwd All Serv	Enable/disable call-forward-all service. Defaults to yes.
Cfwd Busy Serv	Enable/disable call-forward-on-busy service. Defaults to yes.
Cfwd On No Ans Serv	Enable/disable call-forward-on-no-answer service. Defaults to yes.
Paging Serv	Enable/disable the paging service. Defaults to yes.
Call Park Serv	Enable/disable the call park service. Defaults to yes.
Call Pick Up Serv	Enable/disable the call pickup service. Defaults to yes.
ACD Login Serv	Enable/disable the ACD Login Service, used for call centers. Typically enabled with the <SIP-B> parameter. Defaults to no.
Group Call Pick Up Serv	Enable/disable the group call pickup service. Defaults to yes.
Group Call Pick Up Serv	Enable/disable the group call pickup service. Defaults to yes.
ACD Ext	The extension used for handling ACD calls. Select from 1, 2, 3, 4, 5, or 6. Defaults to 1.

Parameter	Description
Service Annc Serv	Enable/disable sending announcement requests to a customer-supplied announcement server. Defaults to no.
Web Serv (Cisco SPA 525G only)	Enable/disable the web server. Defaults to yes.
SMS Serv (Cisco SPA 525G only)	Enable/disable the SMS text messaging server.

Ring Tone (Cisco SPA 500 Series)

Each entry defines a ring tone to be used on the phone, with an ID between 1 and 10. The ID can be used in a DirEntry to indicate which ring tone to use when the corresponding caller calls.

Parameter	Description
Ring1	Ring tone script for ring 1. Defaults to n=Classic-1;w=3;c=1.
Ring2	Ring tone script for ring 2. Defaults to n=Classic-2;w=3;c=2.
Ring3	Ring tone script for ring 3. Defaults to n=Classic-3;w=3;c=3.
Ring4	Ring tone script for ring 4. Defaults to n=Classic-4;w=3;c=4.
Ring5	Ring tone script for ring 5. Defaults to n=Simple-1;w=2;c=1.
Ring6	Ring tone script for ring 6. Defaults to n=Simple-2;w=2;c=2.
Ring7	Ring tone script for ring 7. Defaults to n=Simple-3;w=2;c=3.
Ring8	Ring tone script for ring 8. Defaults to n=Simple-4;w=2;c=4.

Parameter	Description
Ring9	Ring tone script for ring 9. Defaults to n=Simple-5;w=2;c=5.
Ring10	Ring tone script for ring 10. Defaults to n=Office;w=4;c=1.

Ring Tone (WIP310)

Parameter	Description
Keypad Tone	Select yes to enable the keypad tone to be played when a key on the keypad is pressed. Select no to silence the keypad.
Keypad Tone Volume	Corresponds to the volume of the keypad tone. Default is 5.

Auto Input Gain (dB)

NOTE Does not apply to the WIP310.

Parameter	Description
Handset Input Gain	The amount of amplification to apply to the audio input signal for the handset. Defaults to zero.
Headset Input Gain	The amount of amplification to apply to the audio input signal for the headset. Defaults to zero.

Parameter	Description
Speakerphone Input Gain	The amount of amplification to apply to the audio input signal for the speakerphone. Defaults to zero.
Handset Additional Input Gain	Applies additional input gain to the handset.
Headset Additional Input Gain	Applies additional input gain to the headset.
Speakerphone Additional Input Gain	Applies additional input gain to the speakerphone.

Multiple Paging Group Parameters

Parameter	Description
Group Paging Script	You can configure a phone as part of a paging group. Users can then direct pages to specific groups of phones. A phone can be part of no more than two paging groups, and user can page a maximum of five paging groups. The syntax is as follows: pggrp=ip-address:port;[name=xxx;]num=xxx;[listen={yes|no}]]; Where: *IP address*: Multicast IP address of the phone that will listen for and receive pages. *port*: Port on which to page; you must use different ports for each paging group. name (optional): The name of the paging group. num: The number users will dial to access the paging group; must be unique to the group. listen: If the phone should listen on the page group. Only the first two groups with listen set to yes will listen to group pages. If the field is not defined, the default value is no, so you must set this field to listen to the group pages.

Extension Mobility

You can use extension mobility currently with BroadSoft. For more information, see **Configuring Extension Mobility with a BroadSoft Server, page 76**.

NOTE Does not apply to the WIP310.

Parameter	Description
Extension Mobility	Enable or disable extension mobility. Defaults to no (disabled).
EM User Domain	The user domain for extension mobility. Defaults to blank.

BroadSoft Settings

The Cisco SPA 500 Series supports the BroadSoft directory feature and synchronization of Do Not Disturb and Call Forward. The following configuration fields are available:

Parameter	Description
Directory Enable	Set to **yes** to enable BroadSoft directory for the phone user. Defaults to no.
XSI Host Server	Enter the name of the server; for example, xsp.xdp.broadsoft.com.
Directory Name	Name of the directory. Displays on the user's phone as a directory choice.

Parameter	Description
Directory Type	Select the type of BroadSoft directory: ▪ Enterprise (default): Allows users to search on last name, first name, user or group ID, phone number, extension, department, or email address. ▪ Group: Allows users to search on last name, first name, user ID, phone number, extension, department, or email address. ▪ Personal: Allows users to search on last name, first name, or telephone number.
Directory UserID	BroadSoft User ID of the phone user; for example, johndoe@xdp.broadsoft.com.
Directory Password	Alphanumeric password associated with the User ID.
Call Feature Sync Ext	Allows the phone to synchronize with the call server so that if Do Not Disturb or Call Forwarding settings are changed on the phone, changes are also made on the server; if changes are made on the server, they are propagated to the phone. This feature is disabled by default. Choose the extension (1 through 5) that is registered to the BroadSoft server.

XML Service

The Cisco SPA 500 Series supports XML services, such as an XML Directory Service or other XML applications. The following configuration fields are available:

Parameter	Description
XML Directory Service Name	Name of the XML Directory. Displays on the user's phone as a directory choice.
XML Directory Service URL	URL where the XML Directory is located.
XML Application Service	Name of the XML application. Displays on the user's phone as a web application choice.
XML Application Service URL	URL where the XML application is located.

Lightweight Directory Access Protocol (LDAP) Corporate Directory Search

NOTE Does not apply to the WIP310.

If using Active Directory with authentication set to MD5, you must first configure the following:

- Click the **System** tab. In the **Optional Network Configuration** section, under **Primary DNS**, enter the IP address of the DNS server.
- In the **Optional Network Configuration** section, under **Domain**, enter the LDAP domain.

Parameter	Description
LDAP Dir Enable	Choose **yes** to enable LDAP.
LDAP Corp Dir Name	Enter a free-form text name, such as “Corporate Directory.”
LDAP Server	Enter a fully qualified domain name or IP address of LDAP server, in the following format: `nnn.nnn.nnn.nnn`
LDAP Auth Method	Select the authentication method that the LDAP server requires. Choices are: ▪ None—No authentication is used between the client and the server. ▪ Simple—The client sends its fully-qualified domain name and password to the LDAP server. May present security issues. ▪ Digest-MD5—The LDAP server sends authentication options and a token to the client. The client returns an encrypted response that is decrypted and verified by the server.

Parameter	Description

LDAP Client DN	Enter the distinguished name domain components [dc] ; for example:
	`dc=cv2bu,dc=com`
	If using the default Active Directory schema (Name(cn)->Users->Domain), an example of the client DN follows:
	`cn="David Lee",dc=users,dc=cv2bu,dc=com`

LDAP Username	Enter the username for a credentialed user on the LDAP server.
LDAP Password	Enter the password for the LDAP username.
LDAP Search Base	Specify a starting point in the directory tree from which to search. Separate domain components [dc] with a comma. For example: dc=cv2bu,dc=com
LDAP Last Name Filter	This defines the search for surnames [sn], known as last name in some parts of the world. For example, sn:(sn=*$VALUE*). This search allows the provided text to appear anywhere in a name, beginning, middle, or end.
LDAP First Name Filter	This defines the search for the common name [cn]. For example, cn:(cn=*$VALUE*). This search allows the provided text to appear anywhere in a name, beginning, middle, or end.
LDAP Search Item 3	Additional customized search item. Can be blank if not needed.
LDAP Item 3 Filter	Customized filter for the searched item. Can be blank if not needed.
LDAP Search Item 4	Additional customized search item. Can be blank if not needed.
LDAP Item 4 Filter	Customized filter for the searched item. Can be blank if not needed.

Parameter	Description
LDAP Display Attrs	Format of LDAP results display on phone where: ▪ a—Attribute name ▪ cn—Common name ▪ sn—Surname (last name) ▪ telephoneNumber—phone number ▪ n—Display name ▪ t—type ▪ p—phone number
LDAP Number Mapping	Can be blank if not needed. **NOTE** With the LDAP number mapping you can manipulate the number that was retrieved from the LDAP server. For example, you can append 9 to the number if your dial plan requires a user to enter 9 before dialing. If you do not manipulate the number in this fashion, a user can use the **Edit Dial** feature to edit the number before dialing out.

Programmable Softkeys

Parameter	Description
Programmable Softkey Enable	The Cisco SPA 500 Series IP phones have four softkeys on the screen that, when pressed, perform certain actions. (The SPA501 does not have any softkeys.) You can customize the softkeys displayed on the phone, and create your own softkeys for speed dials or XML scripts. Choose **yes** to enable programmable softkeys. The softkey information is entered in the PSK1 through PSK6 fields.
Idle Key List	Softkeys that display when the phone is idle. See **Customizing Phone Softkeys, page 50** for more information.

Parameter	Description
Missed Call Key List	Softkeys that display when a call has been missed. See **Customizing Phone Softkeys, page 50** for more information.
Off Hook Key List	Softkeys that display when the receiver is lifted, or the headphone or speakerphone buttons are pressed. See **Customizing Phone Softkeys, page 50** for more information.
Dialing Input Key List	Softkeys that display when the user must enter dialing data. See **Customizing Phone Softkeys, page 50** for more information.
Progressing Key List	Softkeys that display when a call is attempting to connect. See **Customizing Phone Softkeys, page 50** for more information.
Connected Key List	Softkeys that display when a call is connected. See **Customizing Phone Softkeys, page 50** for more information.
Start-Xfer Key List	Softkeys that display when a call transfer has been initiated. See **Customizing Phone Softkeys, page 50** for more information.
Start-Conf	Softkeys that display when a conference call has been initiated. See **Customizing Phone Softkeys, page 50** for more information.
Conferencing Key List	Softkeys that display when a conference call is in progress. See **Customizing Phone Softkeys, page 50** for more information.
Releasing Key List	Softkeys that display when a call is disconnecting. See **Customizing Phone Softkeys, page 50** for more information.
Hold Key List	Softkeys that display when one or more calls are on hold. See **Customizing Phone Softkeys, page 50** for more information.
Ringing Key List	Softkeys that display when a call is incoming. See **Customizing Phone Softkeys, page 50** for more information.
Shared Active Key List	Softkeys that display when a call is active on a shared line. See **Customizing Phone Softkeys, page 50** for more information.

Parameter	Description
Shared Held Key List	Softkeys that display when a call is on hold on a shared line. See **Customizing Phone Softkeys, page 50** for more information.
PSK1 through PSK6	To configure a speed dial script, enter the following in the PSK field: fnc=sd;ext=*extensionname*@$PROXY;vid=*outbound extnum*;nme=*name* where fnc is the function of the key (speed dial), ext (*extensionname*) is the extension being dialed, *vid* is the extension on the calling phone from which the outbound call is sent, and *name* is the name of the speed dial being configured. To configure an XML script, enter the following in the PSK field: fnc=xml;url=http://*scriptURL.xml*;nme=*scriptname* where fnc is the function of the key (an XML script), *scriptURL.xml* is the URL where the script is located, and *scriptname* is the name of the script.

Ext Tab

The Ext tabs vary by phone and depend on the number of extensions the phone model supports.

This section describes the fields for the following Ext tab headings:

- **General, page 245**
- **Share Line Appearance, page 264**
- **NAT Settings, page 265**
- **Network Settings, page 265**
- **SIP Settings, page 266**
- **Call Feature Settings, page 269**
- **Proxy and Registration, page 271**

- Subscriber Information, page 274
- Audio Configuration, page 275
- Dial Plan, page 278

In a configuration profile, the Line parameters must be appended with the appropriate numeral to indicate the line to which the setting applies. For example:

```
[1] to specify line one
[2] to specify line two
```

General

Line Enable: To enable this line for service, select yes. Otherwise, select no.

Defaults to yes.

Share Line Appearance

Parameter	Description
Share Ext	Indicates whether this extension is to be shared with other stations or private. If the extension is not shared, then a call appearance assigned to this extension is not shared, regardless the setting of <Share Call Appearance> for that call appearance. If the extension is shared, then whether or not a call appearance assigned to this extension is shared follows the setting of <Share Call Appearance> for that call appearance. The choices are shared or private. Defaults to shared.
Shared User ID	The user identified assigned to the shared line appearance.
Subscription Expires	Number of seconds before the SIP subscription expires. Before the subscription expiration, the phone gets NOTIFY messages from the SIP server on the status of the shared phone extension. Defaults to 60 seconds.

NAT Settings

Parameter	Description
NAT Mapping Enable	To use externally mapped IP addresses and SIP/RTP ports in SIP messages, select yes. Otherwise, select no. Defaults to no.
NAT Keep Alive Enable	To send the configured NAT keep alive message periodically, select yes. Otherwise, select no. Defaults to no.
NAT Keep Alive Msg	Enter the keep alive message that should be sent periodically to maintain the current NAT mapping. If the value is $NOTIFY, a NOTIFY message is sent. If the value is $REGISTER, a REGISTER message without contact is sent. Defaults to $NOTIFY.
NAT Keep Alive Dest	Destination that should receive NAT keep alive messages. If the value is $PROXY, the messages are sent to the current or outbound proxy. Defaults to $PROXY.

Network Settings

Parameter	Description
SIP TOS/DiffServ Value	TOS/DiffServ field value in UDP IP packets carrying a SIP message. Defaults to 0x68.
SIP CoS Value	CoS value for SIP messages. Defaults to 3.

Parameter	Description
RTP TOS/DiffServ Value	ToS/DiffServ field value in UDP IP packets carrying RTP data. Defaults to 0xb8.
RTP CoS Value	CoS value for RTP data. Defaults to 6.
Network Jitter Level	Determines how jitter buffer size is adjusted by the IP phone. Jitter buffer size is adjusted dynamically. The minimum jitter buffer size is 30 milliseconds or (10 milliseconds + current RTP frame size), whichever is larger, for all jitter level settings. However, the starting jitter buffer size value is larger for higher jitter levels. This setting controls the rate at which the jitter buffer size is adjusted to reach the minimum. Select the appropriate setting: low, medium, high, very high, or extremely high. Defaults to high.
Jitter Buffer Adjustment	Controls how the jitter buffer should be adjusted. Select the appropriate setting: up and down, up only, down only, or disable. Defaults to up and down.

SIP Settings

Parameter	Description
SIP Transport	Select from UDP, TCP, or TLS. Defaults to UDP.
SIP Port	Port number of the SIP message listening and transmission port. Defaults to 5060.

Parameter	Description
SIP 100REL Enable	To enable the support of 100REL SIP extension for reliable transmission of provisional responses (18x) and use of PRACK requests, select yes. Otherwise, select no. Defaults to no.
EXT SIP Port	The external SIP port number.
Auth Resync-Reboot	If this feature is enabled, the IP phone authenticates the sender when it receives the NOTIFY resync reboot (RFC 2617) message. To use this feature, select yes. Otherwise, select no. Defaults to yes.
SIP Proxy-Require	The SIP proxy can support a specific extension or behavior when it sees this header from the user agent. If this field is configured and the proxy does not support it, it responds with the message, unsupported. Enter the appropriate header in the field provided.
SIP Remote-Party-ID	To use the Remote-Party-ID header instead of the From header, select yes. Otherwise, select no. Defaults to yes.
Referor Bye Delay	Controls when the IP phone sends BYE to terminate stale call legs upon completion of call transfers. Multiple delay settings (Referor, Refer Target, Referee, and Refer-To Target) are configured on this screen. For the Referor Bye Delay, enter the appropriate period of time in seconds. Defaults to 4.
Refer-To Target Contact	To contact the refer-to target, select yes. Otherwise, select no. Default: **no**
Referee Bye Delay	For the Referee Bye Delay, enter the appropriate period of time in seconds. Defaults to 0.

Parameter	Description
SIP Debug Option	SIP messages are received at or sent from the proxy listen port. This feature controls which SIP messages to log. Choices are as follows: ▪ none—No logging. ▪ 1-line—Logs the start-line only for all messages. ▪ 1-line excl. OPT—Logs the start-line only for all messages except OPTIONS requests/responses. ▪ 1-line excl. NTFY—Logs the start-line only for all messages except NOTIFY requests/responses. ▪ 1-line excl. REG—Logs the start-line only for all messages except REGISTER requests/responses. ▪ 1-line excl. OPT|NTFY|REG—Logs the start-line only for all messages except OPTIONS, NOTIFY, and REGISTER requests/responses. ▪ full—Logs all SIP messages in full text. ▪ full excl. OPT—Logs all SIP messages in full text except OPTIONS requests/responses. ▪ full excl. NTFY—Logs all SIP messages in full text except NOTIFY requests/responses. ▪ full excl. REG—Logs all SIP messages in full text except REGISTER requests/responses. ▪ full excl. OPT|NTFY|REG—Logs all SIP messages in full text except for OPTIONS, NOTIFY, and REGISTER requests/responses. Defaults to none.
Refer Target Bye Delay	For the Refer Target Bye Delay, enter the appropriate period of time in seconds. Defaults to 0.
Sticky 183	If this feature is enabled, the IP telephony ignores further 180 SIP responses after receiving the first 183 SIP response for an outbound INVITE. To enable this feature, select yes. Otherwise, select no. Defaults to no.

Parameter	Description
Auth INVITE	When enabled, authorization is required for initial incoming INVITE requests from the SIP proxy.
Ntfy Refer On 1xx-To-Inv	If set to **yes**, as a transferee, the phone will send a NOTIFY with Event:Refer to the transferor for any 1xx response returned by the transfer target, on the transfer call leg. If set to **no**, the phone will only send a NOTIFY for final responses (200 and higher). **NOTE** Not applicable to the WIP310.
Use Anonymous With RPID	This parameter applies only if <SIP Remote-Party-ID> is set to **yes**; otherwise, it is ignored. If the parameter is set to **yes**, the FROM header's display-name and user-id fields are set to anonymous when the caller blocks his caller-id. If the parameter is set to **no**, the FROM header's display-name and user-id are not masked. The Remote-Party-ID header indicates privacy=full when the caller wishes to block his caller-id. Default: yes. **NOTE** Not applicable to the WIP310.
Set G729annexb	Configure G.729 Annex B settings. **NOTE** Not applicable to Cisco SPA 525G.

Call Feature Settings

Parameter	Description
Blind Attn-Xfer Enable	Enables the IP phone to perform an attended transfer operation by ending the current call leg and performing a blind transfer of the other call leg. If this feature is disabled, the IP phone performs an attended transfer operation by referring the other call leg to the current call leg while maintaining both call legs. To use this feature, select **yes**. Otherwise, select **no**. Defaults to no.

Parameter	Description
MOH Server	User ID or URL of the auto-answering streaming audio server. When only a user ID is specified, the current or outbound proxy is contacted. Music-on-hold is disabled if the MOH Server is not specified. Defaults to imusic when used with a Cisco SPA 9000 IP PBX.
Message Waiting	Indicates whether the Message Waiting Indicator on the phone is lit. This parameter is toggled by a message from the SIP proxy to indicate if a message is waiting. You can manually modify it to clear or set the flag in the Ext 1-6 tab. Setting this value to Yes can activate stutter tone and VMWI signal. This parameter is stored in long-term memory and survives after reboot or power cycle. Defaults to No.
Auth Page	Specifies whether to authenticate the invite before auto answering a page. Defaults to No.
Default Ring	Type of ring heard. This corresponds to the Ring Tone on the Phone tab. Choose from No Ring, 1 through 10, User 1, or User 2. Defaults to 1.
Auth Page Realm	Identifies the Realm part of the Auth that is accepted when the Auth Page parameter is set to Yes. This parameter accepts alphanumeric characters. Defaults to blank.
Conference Bridge URL	This is the URL used to join into a conference call, generally in the form of the word “conference” or “user@IPaddress:port”. Defaults to blank.
Auth Page Password	Identifies the password used when the Auth Page parameter is set to Yes. This parameter accepts alphanumeric characters. Defaults to blank.

Parameter	Description
Mailbox ID	Identifies the voice mailbox number/ID for the phone. Defaults to blank.
Voice Mail Server	Identifies the SpecVM server for the phone, generally the IP address and port number of the VM server.
State Agent	Reserved feature.
CFWD Notify Serv	Specifies whether to enable a SIP-B feature regarding the sending of a Notify to the phone when a call is forwarded elsewhere. Defaults to No.
CFWD Notifier	Typically, this field is configured with the SIP proxy information.

Proxy and Registration

Parameter	Description
Proxy	SIP proxy server and port number set by the Service Provider for all outbound requests. For example: 192.168.2.100:6060.

Parameter	Description
Use Outbound Proxy	Enables an outbound proxy (for example, 172.20.2.1:5060—port is optional) or a domain name such as sip.server.com as long as this name is a fully-qualified domain name. If set to no, the Outbound Proxy and Use OB Proxy in Dialog fields are ignored. Defaults to no. Optionally, the proxy can be configured (SPA5xx only) for Survivable Remote Site Telephony (SRST) support. The proxy is configured with an extension that includes a statically-configured DNS SRV record or DNS A record. Configuring the proxy allows for failover and fallback functionality with a secondary proxy server. For example: **For SRV Record:** sip.server.com:SRV=node1.sip.server.com:5060:p=1:w=50lnode2.sip.server.com:5060:p=2:w=50 **NOTE** Set "Use DNS SRV" to **no** and "DNS SRV Auto Prefix" to **no**. **For A Record:** sip.server.com:A=172.20.2.1,172.20.2.2 **NOTE** Set "Use DNS SRV" to **no** and "DNS SRV Auto Prefix" to **no**.
Outbound Proxy	SIP Outbound Proxy Server where all outbound requests are sent as the first hop.
Use OB Proxy In Dialog	Whether to force SIP requests to be sent to the outbound proxy within a dialog. Ignored if <Use Outbound Proxy> is no or <Outbound Proxy> is empty. Defaults to yes.
Register	Enable periodic registration with the <Proxy>. This parameter is ignored if <Proxy> is not specified. Defaults to yes.
Make Call Without Reg	Allow making outbound calls without successful (dynamic) registration by the unit. If no, the dial tone will not play unless registration is successful. Defaults to no.

Parameter	Description
Register Expires	Allow answering inbound calls without successful (dynamic) registration by the unit. If proxy responded to REGISTER with a smaller Expires value, the phone will renew registration based on this smaller value instead of the configured value. If registration failed with an Expires too brief error response, the phone will retry with the value given in the Min-Expires header in the error response. Defaults to 60.
Ans Call Without Reg	If enabled, the user does not have to be registered with the proxy to answer calls. Defaults to no.
Use DNS SRV	Whether to use DNS SRV lookup for Proxy and Outbound Proxy. Defaults to no.
DNS SRV Auto Prefix	If enabled, the phone will automatically prepend the Proxy or Outbound Proxy name with _sip._udp when performing a DNS SRV lookup on that name. Defaults to no.
Proxy Fallback Intvl	This parameter sets the delay (sec) after which the phone will retry from the highest priority proxy (or outbound proxy) servers after it has failed over to a lower priority server. This parameter is useful only if the primary and backup proxy server list is provided to the phone via DNS SRV record lookup on the server name. (Using multiple DNS A record per server name does not allow the notion of priority and so all hosts will be considered at the same priority and the phone will not attempt to fall back after a fail over). Defaults to 3600

Parameter	Description
Proxy Redundancy Method	Select Normal or Based on SRV port. The phone creates an internal list of proxies returned in the DNS SRV records. If you select Normal, the list contains proxies ranked by weight and priority. If you select Based on SRV, the phone uses normal, then inspects the port number based on the first listed proxy port. Defaults to Normal.

Subscriber Information

Parameter	Description
Display Name	Display name for caller ID.
User ID	Extension number for this line.
Password	Password for this line. Defaults to blank.
Use Auth ID	To use the authentication ID and password for SIP authentication, select yes. Otherwise, select no to use the user ID and password. Defaults to no.
Auth ID	Authentication ID for SIP authentication. Defaults to blank.
Mini Certificate	Base64 encoded of Mini-Certificate concatenated with the 1024-bit public key of the CA signing the MC of all subscribers in the group. Defaults to blank.
SRTP Private Key	Base64 encoded of the 512-bit private key per subscriber for establishment of a secure call. Defaults to blank.

Audio Configuration

A codec resource is considered as allocated if it has been included in the SDP codec list of an active call, even though it eventually may not be the one chosen for the connection. So, if the G.729a codec is enabled and included in the codec list, that resource is tied up until the end of the call whether or not the call actually uses G.729a. If the G.729a resource is already allocated and since only one G.729a resource is allowed per device, no other low-bit-rate codec may be allocated for subsequent calls; the only choices are G711a and G711u. On the other hand, two G.723.1/G.726 resources are available per device.

Therefore it is important to disable the use of G.729a in order to guarantee the support of two simultaneous uses of the G.723/G.726 codecs.

Parameter	Description
Preferred Codec	Preferred codec for all calls. (The actual codec used in a call still depends on the outcome of the codec negotiation protocol.) Select one of the following: G711u, G711a, G722, G726-16, G726-24, G726-32, G726-40, G729a, or G723. **NOTE** Cisco SPA 525G choices are: G711u, G711a, G726-32, G729a, and G722. G722 not available on WIP310. Defaults to G711u.
Use Pref Codec Only	To use only the preferred codec for all calls, select yes. (The call fails if the far end does not support this codec.) Otherwise, select no. Defaults to no.
Second Preferred Codec	The second preferred codec when the preferred codec cannot be used. If *Use Pref Codec Only* is enabled (set to **yes**), this parameter is not used. Defaults to Unspecified.
Third Preferred Codec	The third preferred codec when the preferred codec and second preferred codec cannot be used. If *Use Pref Codec Only* is enabled (set to **yes**), this parameter is not used. Defaults to Unspecified.

Parameter	Description
G729a Enable	To enable the use of the G.729a codec at 8 kbps, select yes. Otherwise, select no. Defaults to yes.
G722 Enable	Enables use of the G.722 codec. Defaults to yes. **NOTE** Not applicable to the WIP310.
G723 Enable	To enable the use of the G.723a codec at 6.3 kbps, select yes. Otherwise, select no. Defaults to yes. **NOTE** G.723.1 is not supported on the Cisco SPA 525G or WIP310.
G726-16 Enable	To enable the use of the G.726 codec at 16 kbps, select yes. Otherwise, select no. Defaults to yes. **NOTE** Not supported on the Cisco SPA 525G.
G726-24 Enable	To enable the use of the G.726 codec at 24 kbps, select yes. Otherwise, select no. Defaults to yes. **NOTE** Not supported on the Cisco SPA 525G or WIP310.
L16 Enable	To enable the use of the L16 codec, select yes. Otherwise, select no. Defaults to yes. **NOTE** Cisco SPA 525G only.
G726-32 Enable	To enable the use of the G.726 codec at 32 kbps, select yes. Otherwise, select no. Defaults to yes.
G726-40 Enable	To enable the use of the G.726 codec at 40 kbps, select yes. Otherwise, select no. Defaults to yes. **NOTE** Not applicable to the Cisco SPA 525G.

Parameter	Description
Release Unused Codec	Allows the release of codecs not used after codec negotiation on the first call so that other codecs can be used for the second line. To use this feature, select yes. Defaults to yes.
DTMF Process AVT	Select yes to process RTP DTMF events. Otherwise, select no. If this parameter is set to no, the AVT payload type is not included in outbound SDP. Defaults to yes.
Silence Supp Enable	To enable silence suppression so that silent audio frames are not transmitted, select yes. Otherwise, select no. See **Ensuring Voice Quality, page 114**. Defaults to no.
DTMF Tx Method	Select the method to transmit DTMF signals to the far end: InBand, AVT, INFO, Auto, InBand+INFO, or AVT+INFO. InBand sends DTMF using the audio path. AVT sends DTMF as AVT events. INFO uses the SIP INFO method. Auto uses InBand or AVT based on the outcome of codec negotiation. Defaults to Auto.
DTMF Tx Volume for AVT Packet	Allows you to manually configure the AVT Tx volume. The value of this parameter is inserted into the volume field of the payload in the AVT packet. Values are based on the AVT specification as described in RFC 2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*. According to RFC 2833, the volume field is represented by 6 bits, and describes the power level of the tone, expressed in dBm0 after dropping the sign. Valid range for this parameter is 0 to 63. If the provisioned value is negative, it will be negated first. Thereafter, if the value is beyond the high limit of 63, it will be clipped to 63. The default value is 0, and is the recommended setting. However, some gateways do not accept this volume setting. If the gateway does not accept the value of 0, the DTMF tone is not relayed to the remote end. As a workaround for the phone to interoperate with those gateways, you can change the value to a value greater than 0.

A codec resource is considered allocated if it has been included in the SDP codec list of an active call, even though it eventually might not be chosen for the connection. If the G.729a codec is enabled and included in the codec list, that resource is tied up until the end of the call whether or not the call actually uses G.729a. If the G729a resource is already allocated (and since only one G.729a resource is allowed per phone), no other low-bit-rate codec can be allocated for subsequent calls. The only choices are G711a and G711u.

Since two G.723.1/G.726 resources are available per IP phone, you should disable the use of G.729a to guarantee support for two simultaneous G.723/G.726 codecs.

Dial Plan

The default dial plan script for each line is as follows: (*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxx|xxxxxxxxxxxx.).

Parameter	Description
Dial Plan	Dial plan script for this line. The default is (<9:>xx.) (*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxxx.) The dial plan syntax is expanded in the Cisco SPA to allow the designation of three parameters to be used with a specific gateway: ▪ uid – the authentication user-id ▪ pwd – the authentication password ▪ nat – if this parameter is present, use NAT mapping Each parameter is separated by a semi-colon (;).
Enable IP Dialing	Enable or disable IP dialing. Defaults to no.

User Tab

This section describes the fields for the following headings on the User tab:

Call Forward

Parameter	Description
Cfwd All Dest	Enter the extensions to forward calls to.
Cfwd Busy Dest	Enter the extensions to forward calls to when the line is busy. Defaults to voice mail.
Cfwd No Ans Dest	Enter the extension to forward calls to when the call is not answered. Defaults to voice mail.
Cfwd No Ans Delay	Enter the time delay in seconds to wait before forwarding a call that is not answered. Defaults to 20 seconds.

See Vertical Service Activation Codes, page 230 for more information on call forwarding parameters.

Speed Dial

Speed Dial 2 through 9: Target phone number (or URL) assigned to speed dial 2, 3, 4, 5, 6, 7, 8, or 9.

Defaults to blank.

NOTE Speed dial configuration has its own tab on the Cisco SPA 525G and does not appear in this section on the WIP310. Speed dial configuration from the WIP310 is done on the phone. You can also configure speed dials on the Cisco SPA 500 Series IP phones; see the User Guide for the phone for more information.

Supplementary Services

The IP phone provides native support of a large set of enhanced or supplementary services. All of these services are optional. Most supplementary service parameters are listed in **Supplementary Services, page 252**.

The user can enable or disable supplementary services and other settings in this section.

A supplementary service should be disabled if the user has not subscribed for it, or the service provider intends to support similar service using other means.

For more star code or supplementary service information, see **Configuring Supplementary Services (Star Codes), page 153**.

Camera Settings

The Cisco SPA 525G works with the Cisco WVC2300 Wireless-G Business Internet Video Camera and the Cisco PVC2300 Business Internet Video Camera to provide simple video monitoring from your IP phone. See **Entering Camera Information Into the Cisco SPA525G Web Administration Interface, page 78**.

Web Information Service Settings (Cisco SPA 525G)

NOTE These parameters apply only to the Cisco SPA 525G.

For configuration information, see **Configuring RSS Newsfeeds on the Cisco SPA 525G IP Phone, page 61**.

Audio Volume

NOTE Does not apply to the WIP310.

Parameter	Description
Ringer Volume	Sets the default volume for the ringer.
Speaker Volume	Sets the default volume for the full-duplex speakerphone.
Handset Volume	Sets the default volume for the handset.
Headset Volume	Sets the default volume for the headset.
Bluetooth Volume	Volume of the Bluetooth device. **NOTE** Applies to the Cisco SPA 525G only.

Screen (Cisco SPA 525G)

Parameter	Description
Screen Saver Enable	Enables a screen saver on the phone's LCD. When the phone is idle for a specified time, it enters screen saver mode. (Users can set up screen savers directly using phone Setup button.) Any button press or on/off hook event triggers the phone to return to its normal mode. (The screen shows "Press any key to unlock your phone.") If a user password is set, the user must enter it to exit screen saver mode.

Parameter	Description
Screen Saver Type	Choose the type of screen saver: ▪ **Black Background**—Displays a black screen. ▪ **Gray Background**—Displays a gray screen. ▪ **Black/Gray Rotation**—The screen incrementally cycles from black to gray. ▪ **Picture Rotation**—The screen rotates through available pictures on the phone. ▪ **Digital Frame**—Shows the background picture.
Screen Saver Trigger Time	Number of seconds that the phone remains idle before the screen saver turns on.
Screen Saver Refresh Time	Number of seconds before the screen saver should refresh (if, for example, you chose a rotation of pictures).

Text Logo	Text logo to display when the phone boots up. A service provider, for example, can enter logo text as follows:
	▪ Up to 2 lines of text
	▪ Each line must be fewer than 32 characters
	▪ Insert a new line character (\n) between lines
	▪ Insert escape code %0a
	For example, “Super\n%0aTelecom” will display:
	`Super`
	`Telecom`
	For more information, see the **“Configuring Phone Information and Display Settings” section on page 32.**

BMP Picture Download URL	URL locating the bitmap (.BMP) or .jpg file to display on the LCD background. For more information, see the **“Configuring Phone Information and Display Settings” section on page 32.**
Logo Type	Select from Default, Download BMP Picture, or Text Logo. Defaults to Default. For more information, see the **“Configuring Phone Information and Display Settings” section on page 32.**

Parameter	Description
Background Picture Type	Select from Default, Download BMP Picture, or None. Defaults to Default. For more information, see the **"Configuring Phone Information and Display Settings" section on page 32.**
LCD Contrast	Enter a number value from 1 to 30. The higher the number, the greater the contrast on the screen.
Back Light Enable	Select yes to enable the screen back light.
Back Light Timer (sec)	Enter the number of seconds before the back light should turn off.

Attendant Console Tab (Cisco SPA 500 Series)

This tab includes the following sections:

General

Parameter	Description
Subscribe Expires	Specifies how long the subscription remains valid. After the specified period of time, elapses, the Cisco SPA 500S initiates a new subscription. Defaults to 1800.
Subscribe Retry Interval	Specifies the length of time to wait to try again if subscription fails.
Unit 1 Enable	Enables or disables the first Cisco SPA 500S unit (each IP phone can have up to two Cisco SPA 500Ss attached).

Parameter	Description
Subscribe Delay	Length of delay before attempting to subscribe. Defaults to 1.
Unit 2 Enable	Enables or disables the second Cisco SPA 500S unit (each IP phone can have up to two Cisco SPA 500Ss attached).
Server Type	Selects the type of server used (Cisco SPA 9000, BroadSoft, or Asterisk).
Test Mode Enable	Enables or disables test mode. When test mode is enabled, the LEDs are turned on when keys are pressed, going from off to green to red, and back to off. In test mode, when all the buttons on the Cisco SPA 500S are returned to off, all the keys become orange. The IP phone must be rebooted after the test is completed.
Attendant Console Call Pickup Code	The star code used for picking up a ringing call. Defaults to *98.
BLF List URI	Automatically configures BLF subscriptions for all users on a monitored list. See **Configuring BroadSoft Busy Lamp Field Auto-Configuration, page 189**.
Unit 1 Key 1-32	Enter a strings that define the extension and other parameters associated with each lighted button on the first Cisco SPA 500S unit. Keywords and values are case-sensitive. The configuration script is described in the **"Unit/Key Configuration Scripts" section on page 186**.

For more information, see **Chapter 9, "Configuring the Cisco SPA 500S Attendant Console."**.

Unit 2

See the description for Unit 1 above. Enter a strings that define the extension and other parameters associated with each lighted button on the second Cisco SPA 500S unit. Keywords and values are case-sensitive. The configuration script is described in the **"Setting Up the Cisco SPA 500S Attendant Console" section on page 182**.

Attendant Console Status

This page provides two tabs to display the status of up to two Cisco SPA 500S units that are supported by a single IP phone:

- Unit 1—Displays information about the first Cisco SPA 500S unit.
- Unit 2—Displays information about the second Cisco SPA 500S unit.

Each tab provides the read-only fields described in the following table:

Parameter	Description
Unit Enable	Displays if the Unit is enabled or disabled.
Subscribe Expires	Displays when the current subscription expires. After the subscription expires, the Cisco SPA 500S automatically requests a new subscription.
HW Version	Displays the version of the hardware.
Unit Online	Displays whether the unit is powered on and connected or not.
Subscribe Retry Interval	Displays the length of time the Cisco SPA 500S waits to try again if subscription fails.
SW Version	Displays the version of the software currently running on the unit.
Key Name	Displays the name assigned to each key (1-32) on the Cisco SPA 500S unit.
Type	Displays the function enabled for each key (1-32) on the Cisco SPA 500S unit.
Line	Displays the extension assigned to each key (1-32) on the Cisco SPA 500S unit.
Station	Displays the subscribe URI configured for each key (1-32) on the Cisco SPA 500S unit.

Cisco SPA 525G-Specific Tabs

The following tabs appear on the Cisco SPA 525G.

Wi-Fi

Enable or disable the Wireless-G device from this tab.

Parameter	Description
Wireless Enable	Click **On** to enable the wireless controller.
Wi-Fi Device	Choose the method of wireless setup: ▪ Wi-Fi Profile—Create a wireless profile by manually entering information. ▪ Wi-Fi Protected Setup—If your router has a WPS button, you can use Wi-Fi Protected Setup to add a new wireless network profile.
Wireless Status	Contains information about the wireless network.
Wi-Fi Profile	Contains up to 3 wireless profiles for the phone. Includes a wireless profile for the Cisco Unified Communications Server by default.

Bluetooth (Cisco SPA 525G)

Enable Bluetooth on the Cisco SPA 525G by clicking **On**.

Personal Address Book

Address book for the phone. For more information, see the *Cisco Small Business Pro IP Phone SPA 525G User Guide*.

Call History

Displays the call history for the phone. To change the information displayed, select the type of call history from the drop-down list:

- All Calls
- Received Calls
- Placed Calls
- Missed Calls

Speed Dials

See **Speed Dial, page 280**.

Firmware Upgrade

Used to upgrade the firmware for the Cisco SPA 525G. See **Upgrading Firmware, page 7**.

C

Where to Go From Here

Cisco provides a wide range of resources to help you obtain the full benefits of the Cisco SPA500 Series and Wireless IP Phones.

Product Resources

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads, and enter the model number in the Software Search box.
Product Documentation	
IP Phone	www.cisco.com/en/US/products/ps10499/tsd_products_support_series_home.html
Accessories	www.cisco.com/en/US/products/ps10042/tsd_products_support_series_home.html
Cisco SPA 9000 Voice System	www.cisco.com/en/US/products/ps10030/tsd_products_support_series_home.html

Cisco Unified Communications 500 Series for Small Business	www.cisco.com/en/US/products/ps7293/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace

NOTE For older Cisco IP phone models, such as the Cisco SPA9XX, see the *Cisco SPA9XX Phone Administration Guide* on cisco.com. This guide covers only the Cisco SPA 500 Series IP phones and the Cisco WIP310.